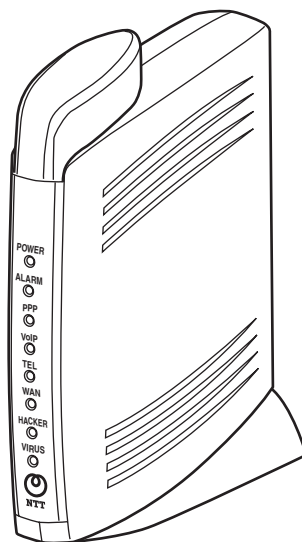
Web Caster X400V
詳細取扱説明書

このたびは、Web Caster X400Vをお買い求めいただきまして、まことにありがとうございます。

●ご使用の前に、この「詳細取扱説明書」をよくお読みのうえ、内容を理解してからお使いください。
●お読みになったあとも、本商品のそばなどいつも手もとに置いてお使いください。

技術基準適合認証品

目 次

目次 ……………………………………………………2
マニュアルの見かた ……………………………………5
マニュアルの見かた ……………………………………5

1 こんなときにはこの設定

こんなときにはこの設定 …………………………………1-2
PPPoEマルチセッションを利用するには……………………1-2
音声／ビデオチャット等のソフトを利用するには…………1-5
インターネットにサーバを公開するには（静的NAPT機能）……1-6
インターネットにサーバを公開するには（簡易DMZ機能）……1-10
複数の固定IPアドレス（Unnumbered）サービスを利用するには ·1-12
LAN側のパソコンにIPアドレスを自分で設定するには…………1-14
LAN側のIPアドレスを変更するには……………………1-15
特定のパソコンのインターネット接続を規制するには …………1-16
スタティックルーティングをするには ……………………1-17
IPv6フレームをブリッジするには…………………………1-19
特定の相手からの呼び出しを拒否するには ………………1-20
LAN側に接続したパソコンのファイルやプリンタを共有するには ··1-20

2 詳細設定方法

Webブラウザによる設定について ……………………………2-2
機能 ……………………………………………………2-2
操作の流れ ……………………………………………2-3
ボタンについて ………………………………………2-4
ご利用方法 ……………………………………………2-5
かんたん設定（オンライン登録含む）…………………2-6
ルータ設定 ……………………………………………2-7
ネットワーク設定 ……………………………………2-8
PPPoE設定 …………………………………………2-11
DHCP設定 …………………………………………2-14
NAPT設定 …………………………………………2-17
IPフィルタ設定 ……………………………………2-20
ルーティングテーブル設定
ルーティング条件（メインセッション）………………2-22
ルーティングテーブル設定
ルーティング条件（サブセッション）…………………2-24
RIP設定………………………………………………2-27
VPNパススルー設定…………………………………2-28
SPI（ステートフルパケットインスペクション）設定…………2-30
Dynamic DNS設定 …………………………………2-32
Windows共有フィルタ/ステルス設定 ……………………2-34
無線LAN設定 …………………………………………2-35

目　次

基本設定 …… 2-36
暗号化設定 …… 2-36
MACアドレスフィルタリング …… 2-37
セキュリティ …… 2-39
ウイルス対策設定 …… 2-40
アップデート設定 …… 2-41
電話設定 …… 2-42
サービス設定 …… 2-43
IP電話設定情報 …… 2-46
状態表示1 …… 2-48
状態表示2 …… 2-51
ログ表示 …… 2-57
障害ログ表示 …… 2-58
通話ログ表示 …… 2-58
不正アクセスログ表示 …… 2-59
ウイルスログ表示 …… 2-59
アップデートログ表示 …… 2-60
保守 …… 2-61
パスワード設定 …… 2-62
Ping送信 …… 2-63
設定値表示 …… 2-63
ファームウェア更新 …… 2-63
自動アップデート …… 2-63
再起動 …… 2-64
Webブラウザによる設定の終了 …… 2-64
セキュリティ設定 …… 2-65

3　無線LANを利用する

LANケーブルを使用した設定 …… 3-2
本商品とパソコンの設定 …… 3-4
①本商品とパソコンを接続する …… 3-4
②本商品に無線LANカードを装着する …… 3-5
③本商品に暗号化を設定する …… 3-6
④本商品の無線LAN設定を確認する …… 3-11
⑤パソコンに無線LANカードのドライバをインストールする …… 3-13
⑥インストールの状態を確認する …… 3-18
⑦パソコンからアクセスポイント（本商品）へ通信する（インフラストラクチャ・モード） …… 3-20
⑧無線LANカードに暗号化を設定する …… 3-26
⑨無線LAN接続を確認する …… 3-30
⑩必要に応じて本商品と無線LANカードの設定を変更する …… 3-30
⑪無線LAN設定を終了する …… 3-30
LANケーブルを使用しない設定 …… 3-31

4 お困りのときには

トラブルや疑問点がある場合 …… 4-2
設定に関するトラブル …… 4-2
通話/ダイヤルに関するトラブル …… 4-3
パソコンに関するトラブル …… 4-4
ウイルス/不正アクセスに関するトラブル …… 4-6
無線LANに関するトラブル …… 4-9
バージョンアップに関するトラブル …… 4-10
その他のトラブル …… 4-11

5 付録

機能仕様 …… 5-2
電話機能 …… 5-2
ルータ機能 …… 5-4
無線機能 …… 5-8
セキュリティ機能 …… 5-8
その他 …… 5-9
用語集 …… 5-12
索引 …… 5-25
設定記入シート …… 5-27

マニュアルの見かた

本商品のマニュアルの見かたについて説明します。

マニュアルの見かた

本書は下記のように構成されています。

1 こんなときにはこの設定

本商品の機能を使うときの設定方法について説明します。
（音声／ビデオチャット等のソフトを利用するには他）

2 詳細設定方法

本商品のデータ設定、状態確認などの保守方法について説明します。Webブラウザを使用します。
かんたん設定やルータ、電話、無線LAN、セキュリティ関連などの各種設定、状態表示、ログ表示などのメニューがあります。メニューをクリックすると各種設定画面が表示されます。この章では画面単位で用途や操作方法について説明します。

3 無線LANを利用する

本商品を無線LANのアクセスポイントとして使用する場合の設定について説明しています。

4 お困りのときには

本商品がうまく動かない、操作しても違う結果になるなど、お困りのときにはこちらをお読みください。

5 付録

本商品のサービス機能について説明します。
また、付録として用語集、設定記入シートを載せましたので活用してください。

ワンポイント

- 本書ではWindows® XP（サービスパック1）の画面を使用して本商品の説明をしています。
- 本書ではOSやブラウザのバージョン、サービスパックについては、2005年10月時点を基準に記載しています。
- お使いになっているパソコンのOSや画面設定によっては表示が異なる場合があります。

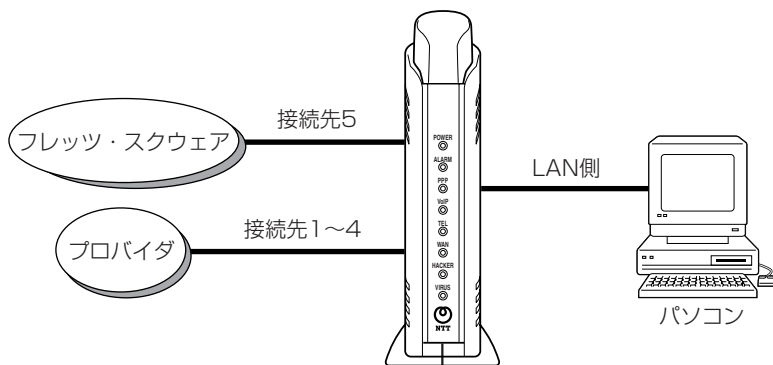
1 こんなときにはこの設定

本章では、いろいろなケースにおける本商品の具体的な設定方法について説明しています。

こんなときにはこの設定 ・・・・・・・・・・・・1-2
PPPoEマルチセッションを
利用するには ・・・・・・・・・・・・・・・・・・・・1-2
音声／ビデオチャット等のソフト
を利用するには ・・・・・・・・・・・・・・・・・1-5
インターネットにサーバを公開するには
（静的NAPT機能）・・・・・・・・・・・・・・1-6
インターネットにサーバを公開するには
（簡易DMZ機能）・・・・・・・・・・・・・1-10
複数の固定IPアドレス（Unnumbered）
サービスを利用するには・・・・・・・1-12
LAN側のパソコンにIPアドレスを
自分で設定するには・・・・・・・・・・・1-14
LAN側のIPアドレスを
変更するには・・・・・・・・・・・・・・・・・・1-15
特定のパソコンのインターネット
接続を規制するには・・・・・・・・・・・1-16
スタティックルーティングを
するには・・・・・・・・・・・・・・・・・・・・・・・1-17
IPv6フレームをブリッジ
するには・・・・・・・・・・・・・・・・・・・・・・・1-19
特定の相手からの呼び出しを
拒否するには・・・・・・・・・・・・・・・・・・1-20
LAN側に接続したパソコンのファイルや
プリンタを共有するには・・・・・・・1-20

こんなときにはこの設定

PPPoEマルチセッションを利用するには

取扱説明書「かんたん設定」で、「インターネットサービスプロバイダ設定」に契約しているプロバイダの情報が設定されていることを前提とします。
複数のプロバイダをご利用になる場合、通常、接続先を切り替える必要があります。PPPoEマルチセッション機能を使うことで、2つ以上のネットワークに同時に接続することができ、接続先の切り替えなしで異なるネットワークがご利用になれます。

※接続先5（フレッツ・スクウェア固定）の接続情報は初期設定で設定されます。変更はできません。（取扱説明書「かんたん設定」）
※NTT東日本エリアをご利用の場合、同時接続できる接続先は2つまでです。（「接続先1～4」のいずれか1つと「接続先5（フレッツ・スクウェア）」になります。）

1 使用する接続先を選択する

Webブラウザで本商品にログインし、メニューの「ルータ設定」－「PPPoE設定」をクリックし、「契約セッション数」と「使用するセッション」を選択します。ここでは「接続先2」を新たに接続する場合で説明します。

PPPoE設定 ヘルプ？

セッション設定

契約セッション数	3	【注意】 PPPoEセッションを3つ以上設定する場合は、以下のホームページにてお客様の契約回線の最大のPPPoEセッション数をご確認の上設定願います。 お客様の契約数以上の設定を行った場合は正常に動作せず、フレッツ・セーフティの機能をご利用出来なくなります。 （NTT東日本エリア / NTT西日本エリア）			
接続先	1	2	3	4	5
メインセッション	◉	○	○	○	○
使用するセッション	☑	☑	☐	☐	☑

2 接続先の接続情報を設定する

接続に必要な手順1で選択した各接続先の接続情報を入力します。

①プロバイダから指定された接続ユーザ名と接続パスワードを入力してください。
「接続パスワード確認」には、確認のため接続パスワードを入力してください。
②「無通信監視タイマ」で「無効」を選択してください。
③プロバイダからDNSサーバアドレスを指定された場合は、そのアドレスを入力してください。
④Unnumbered接続の場合はIPアドレス指定で「指定する（unnumbered接続）」を選択し、プロバイダから割り当てられた固定IPアドレスを入力してください。

⑤「確認」をクリックしてください。入力が不正でなければ「送信」が有効になります。
⑥「送信」をクリックしてください。

3 接続先の接続情報を設定する

接続に必要な手順1で選択した接続先の接続情報を入力します。

①プロバイダから指定されたドメイン名を入力してください。
②手順1で選択した接続先を選択してください。
③「追加」をクリックしてください。

④「確認」をクリックしてください。入力が不正でなければ「送信」が有効になります。
⑤「送信」をクリックしてください。
⑥「反映」をクリックしてください。（ここで接続情報が設定されます。）

（次ページに続く）

こんなときにはこの設定

接続状態を確認する

メニューの「状態表示2」をクリックします。
「PPPoE状態」で、手順2で設定した接続先の状態がそれぞれ「正常」と表示されていれば、マルチセッションで接続されている状態です。

PPPoE状態

	接続／切断	状態
接続先1	接続 切断	正常
接続先2	接続 切断	正常
接続先3	接続 切断	未使用
接続先4	接続 切断	未使用
接続先5		正常

お知らせ

●手順2で「無通信監視タイマ」が「無効」に設定されていないときは、「未使用」と表示される場合があります。実際にインターネット接続を行って接続状態を確認してください。

※本商品のPPPランプを確認してください。

ランプ の種別	ランプのつきかた（色）
PPPランプ	点灯（緑）：1セッション接続時 点灯（橙）：2セッション以上接続時

※接続できなかった場合は、手順1～3をもう一度確認してください。

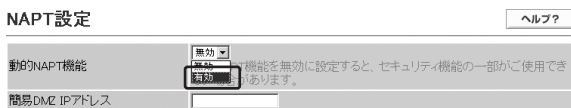
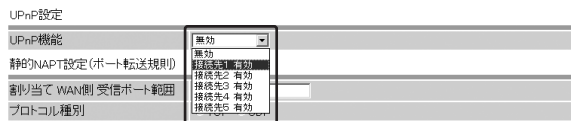
音声／ビデオチャット等のソフトを利用するには

パソコンにインストールしている音声／ビデオチャットソフト等をご利用になる場合は、本商品にUPnP機能の設定をする必要があります。また、ご利用になるソフトのヘルプなどもあわせてご確認ください。

1 「動的NAPT機能」を有効にする

Webブラウザで本商品にログインし、メニューの「ルータ設定」－「NAPT設定」をクリックし、「動的NAPT機能」が「有効」になっていることを確認してください。「無効」になっている場合は、「有効」を選択してください。

NAPT設定

動的NAPT機能	無効
簡易DMZ IPアドレス	

2 「UPnP機能」を利用する接続先を選択する

①「UPnP機能」のプルダウンから利用したい接続先の有効を選択します。
※「UPnP機能」は1つの接続先しか利用できません。

②「確認」をクリックしてください。
③「送信」をクリックしてください。
④「反映」をクリックしてください。

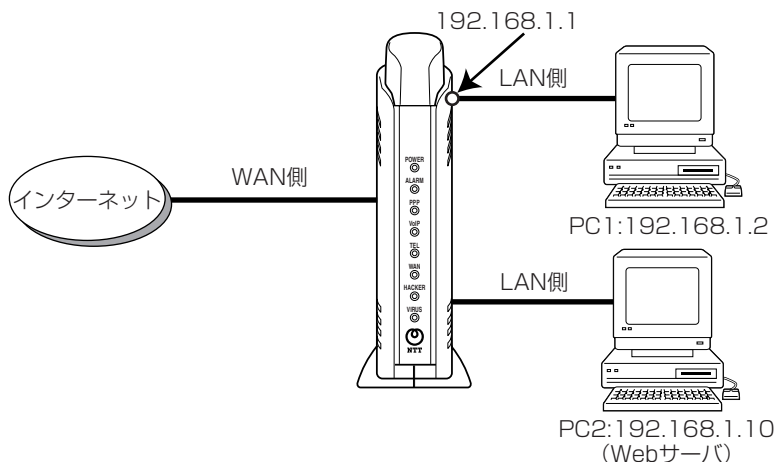
お知らせ

- 「UPnP機能」を「有効」に設定すると、セキュリティ機能の一部が利用できない場合があります。（取扱説明書「セキュリティに関するご注意」）
- 本商品はすべての音声／ビデオチャット等のソフトウェアの動作を保証するものではありません。
- Windows® XP以外のOSでUPnP機能をご利用になる場合は、お使いのパソコンにUPnPドライバがインストールされていることをご確認ください。

こんなときにはこの設定

インターネットにサーバを公開するには（静的NAPT機能）

■Web（HTTP）サーバを公開する場合

Web（HTTP）サーバとして公開するパソコンを用意する必要があります。
以下の接続例では、「PC1」を通常のパソコン（IPアドレス：192.168.1.2)、「PC2」をWebサーバ用のパソコン（IPアドレス：192.168.1.10）としています。サーバを公開するには、「PC2」のIPアドレスを常に固定する設定が必要です。
手順１ではIPアドレスを設定するための「DHCP設定」の設定例を説明します。手順2でサーバを公開するための「NAPT設定」の設定例を説明します。

1 Web（HTTP）サーバとして公開するパソコンのIPアドレスを設定する

Webブラウザで本商品にログインし、メニューの「ルータ設定」－「DHCP設定」をクリックします。

①「LAN側IPアドレス」に本商品のLAN側IPアドレスを入力し、「マスク長」にクラスCのマスク長「24」を入力してください。（例：192.168.1.1）
②「DHCPサーバ機能」を「有効」にしてください。
③「割り当て開始IPアドレス」と「割り当て終了IPアドレス」はクラスCの範囲で①「LAN側IPアドレス」以外（例：192.168.1.2～192.168.1.11）を入力してください。
④「DNSサーバアドレス」は①「LAN側IPアドレス」（例：192.168.1.1）を入力してください。
⑤「IPアドレス」はWebサーバを公開するパソコン（PC2）用に③「割り当て開始IPアドレス」～「割り当て終了IPアドレス」の範囲で入力してください。（例：192.168.1.10）
⑥「MACアドレス」は「Physical Address」の値を入力してください。「Physical Address」の値は「ipconfig /all」などのネットワーク状況を確認するコマンドを実行することで確認できます。
⑦「追加」をクリックしてください。

⑧「確認」をクリックしてください。
⑨「送信」をクリックしてください。
⑩「反映」をクリックしてください。

（次ページに続く）

こんなときにはこの設定

2 インターネットからWeb（HTTP）サーバにアクセスするための設定をする

メニューの「ルータ設定」－「NAPT設定」をクリックします。

①「動的NAPT機能」を「有効」にしてください。
②「割り当てWAN側受信ポート範囲」にWebサーバのポート範囲の「80～80」を入力してください。
③「プロトコル種別」は「TCP」を選択してください。
④「LAN側転送IPアドレス」に手順1で設定したWebサーバとして公開するパソコンのIPアドレス（例：192.168.1.10）を入力してください。
⑤「LAN側転送ポート」にWebサーバのポート「80」を入力してください。
⑥「追加」をクリックしてください。

⑦「確認」をクリックしてください。
⑧「送信」をクリックしてください。
⑨「反映」をクリックしてください。

■FTPサーバを公開する場合

FTPサーバとして公開するパソコンを用意する必要があります。構成例と手順は「Web（HTTP）サーバを公開する場合」と同様になります。

1 FTPサーバとして公開するパソコンのIPアドレスを設定する

※「Web（HTTP）サーバを公開する場合」の手順1（☛P1-7）と同様です。

2 インターネットからFTPサーバにアクセスするための設定をする

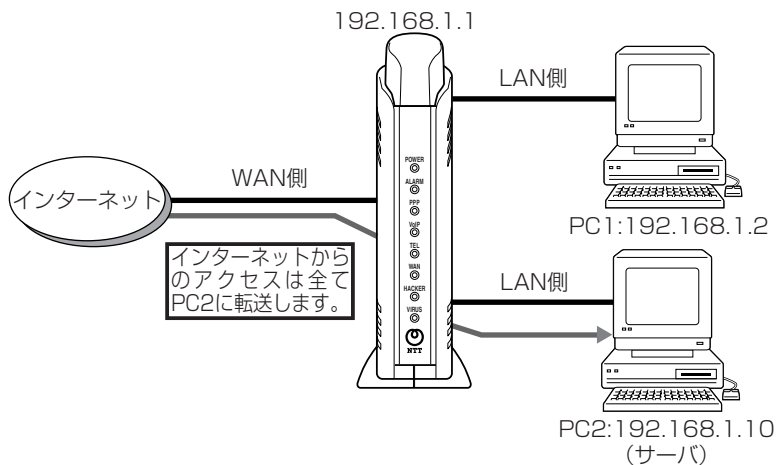
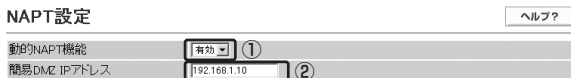
メニューの「ルータ設定」－「NAPT設定」をクリックします。

①「動的NAPT機能」を「有効」にしてください。
②「割り当てWAN側受信ポート範囲」にFTPサーバのポート範囲の「20～21」を入力してください。
③「プロトコル種別」は「TCP」を選択してください。
④「LAN側転送IPアドレス」に手順1で設定したFTPサーバとして公開するパソコンのIPアドレス（例：192.168.1.10）を入力してください。
⑤「LAN側転送ポート」にFTPサーバのポート「20」を入力してください。
⑥「追加」をクリックしてください。

⑦「確認」をクリックしてください。
⑧「送信」をクリックしてください。
⑨「反映」をクリックしてください。

こんなときにはこの設定

インターネットにサーバを公開するには（簡易DMZ機能）

本商品ではインターネットからのアクセスをすべて１台のパソコンに転送する簡易DMZ機能を利用することができます。この機能を利用することにより、インターネットにサーバを公開するための設定が簡単にできます。
以下の接続例では、「PC1」を通常のパソコン（IPアドレス：192.168.1.2)、「PC2」をサーバを公開するパソコン（IPアドレス：192.168.1.10）としています。サーバを公開するには、「PC2」のIPアドレスを常に固定する設定が必要です。

1 サーバとして公開するパソコンのIPアドレスを設定する

※「インターネットにサーバを公開するには（静的NAPT機能）」の「Web（HTTP）サーバを公開する場合」の手順1（☛P1-7）と同様です。

2 インターネット側からサーバにアクセスするための設定をする

メニューの「ルータ設定」－「NAPT設定」をクリックします。

①「動的NAPT機能」が「有効」になっていることを確認してください。「無効」になっている場合は、「有効」を選択してください。
②「簡易DMZ IPアドレス」に手順1で設定したサーバとして公開するパソコンのIPアドレス（例：192.168.1.10）を入力してください。

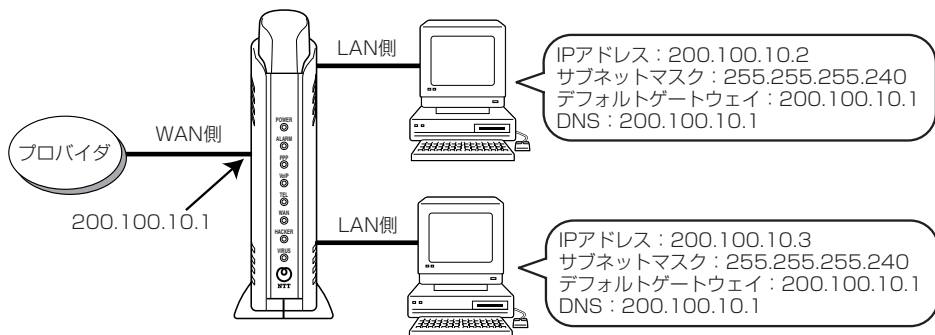
③「確認」をクリックしてください。
④「送信」をクリックしてください。
⑤「反映」をクリックしてください。

お知らせ

●簡易DMZ機能を利用すると、セキュリティ機能の一部が利用できない場合があります。（取扱説明書「セキュリティに関するご注意」）
●本商品の簡易DMZ機能は、お客様のパソコン上で、すべてのソフトウェアの動作を保証するものではありません。

こんなときにはこの設定

複数の固定IPアドレス（Unnumbered）サービスを利用するには

プロバイダから固定IPアドレスが複数割り当てられる（Unnumbered）サービスをご利用の場合のみ利用可能です。
以下の接続例は、Unnumbered接続で、割り当てられたIPアドレスが「200.100.10.0/28」、本商品に設定するIPアドレスが「200.100.10.1」の場合になります。なお、LAN側に接続するパソコンにも設定が必要になります。以下に設定例を示しましたので、こちらも忘れずに設定してください。

1 「セッション設定」をする

Webブラウザで本商品にログインし、「ルータ設定」－「PPPoE設定」をクリックします。
Unnumbered接続で使用する接続先を「使用するセッション」から選択し、「使用するセッション」に合わせて「契約セッション数」を設定します。

PPPoE設定　　ヘルプ?

セッション設定

契約セッション数	2	【注意】 PPPoEセッションを3つ以上設定する場合は、以下のホームページにてお客様の契約回線の最大のPPPoEセッション数をご確認の上設定願います。 お客様の契約数以上の設定を行った場合は正常に動作せず、フレッツ・セーフティの機能をご利用出来なくなります。 （NTT東日本エリア / NTT西日本エリア）			
接続先	1	2	3	4	5
メインセッション	◉	○	○	○	○
使用するセッション	☑	☑	☐	☐	☑

2 接続ユーザ名と接続パスワードを入力する

手順1で選択した接続先にプロバイダから指定された接続ユーザ名と接続パスワードを入力します。
「接続パスワード確認」には、確認のため接続パスワードを入力してください。

インターネットサービスプロバイダ設定
接続先1

接続ユーザ名	
接続パスワード	
接続パスワード確認	

3 「DNSサーバアドレス」を入力する

プロバイダからDNSサーバアドレスを指定された場合は、「DNSサーバアドレス」にそのアドレスを入力します。（例：プライマリ「200.100.10.100」、セカンダリ「200.100.10.200」）

インターネットサービスプロバイダ設定

接続先1

接続ユーザ名	
接続パスワード	
接続パスワード確認	
認証方式	○認証なし ○PAP ○CHAP ⊙PAP+CHAP
無通信監視タイマ	無効
DNSサーバアドレス	プライマリ 200.100.10.100 セカンダリ 200.100.10.200

4 IPアドレスを入力する

①「IPアドレス指定」は「指定する（unnumbered接続）」を選択し、「IPアドレス/マスク長」にプロバイダから割り当てられたIPアドレスを入力します。（例：200.100.10.1/28）

②「確認」をクリックしてください。

③「送信」をクリックしてください。

④「反映」をクリックしてください。

お知らせ

● Unnumbered接続すると、セキュリティ機能のうち、不正アクセスをブロックする機能の一部が利用できません。（取扱説明書「セキュリティに関するご注意」）

こんなときにはこの設定

LAN側のパソコンにIPアドレスを自分で設定するには

本商品の「DHCP設定」の「固定IPアドレスで使用する端末の情報設定」を使用することで常にIPアドレスを一定にすることができます。(「DHCP設定」(☛P2-14))
ここではLAN側のパソコンに設定するIPアドレスが「192.168.1.10」の場合を例に説明します。
Webブラウザで本商品にログインし、メニューの「ルータ設定」－「DHCP設定」をクリックします。

①「LAN側ネットワーク設定」の「LAN側IPアドレス／マスク長」は「192.168.1.1／24」を入力します。
②「固定IPアドレスで使用する端末の情報設定」の「IPアドレス」は「192.168.1.10」、「MACアドレス」はご使用のパソコンのMACアドレスを入力します。
※Windows® 系パソコンのMACアドレスの調べ方はコマンドプロンプトで「winipcfg」または「ipconfig /all」と入力し、「Physical Address」の値になります。
③「追加」をクリックしてください。一覧に設定したデータが追加されます。

④「確認」をクリックしてください。
⑤「送信」をクリックしてください。
⑥「反映」をクリックしてください。
⑦ご使用のパソコンを再起動してください。
⑧設定したIP アドレスになっているか確認してください。

LAN側のIPアドレスを変更するには

本商品の「DHCP設定」の「LAN側ネットワーク設定」で変更することができます。
(「DHCP設定」(☛P2-14))

ここではIPアドレスを「192.168.1.1」から「192.168.10.1」に変更する場合を例に説明します。
Webブラウザで本商品にログインし、メニューの「ルータ設定」－「DHCP設定」をクリックします。

①「LAN側ネットワーク設定」の「LAN側IPアドレス／マスク長」は「192.168.10.1／24」を入力します。
※Webブラウザのアドレス欄に設定するアドレス値が変更になります。
②「DHCPサーバ設定」を以下のように設定します。
・DHCPサーバ機能：有効
・割り当て開始IPアドレス：192.168.10.2
・割り当て終了IPアドレス：192.168.10.10
・DNSサーバアドレス：192.168.10.1

③「確認」をクリックしてください。
④「送信」をクリックしてください。
⑤「反映」をクリックしてください。
⑥ご使用のパソコンを再起動してください。
⑦設定したIP アドレスになっているか確認してください。

こんなときにはこの設定

特定のパソコンのインターネット接続を規制するには

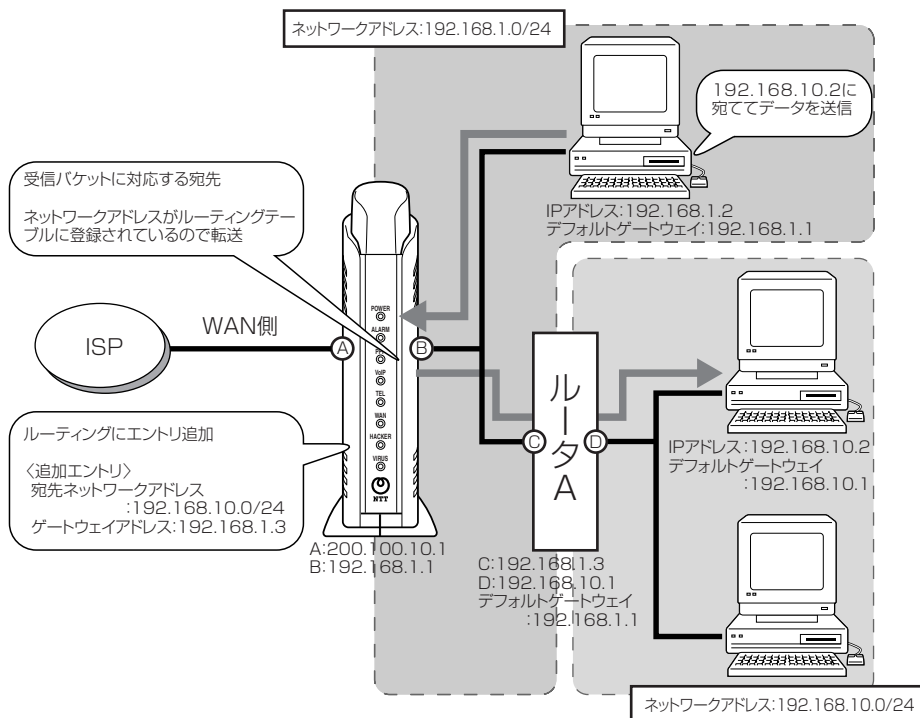
本商品の「IPフィルタ設定」の「パケットフィルタ規則」を使用することで複数接続されたパソコンのうちインターネットにアクセスできないパソコンを指定することができます。
(「IPフィルタ設定」(☛P2-20))

ここでは、「192.168.1.4」と「192.168.1.5」を割り当てたパソコンをインターネットのFTPサーバにアクセスさせない場合を例に説明します。
Webブラウザで本商品にログインし、メニューの「ルータ設定」－「IPフィルタ設定」をクリックします。

①「方針」は「破棄」を選択します。
②「プロトコル種別」は「TCP」を選択します。
③「入力インタフェース」は「LAN」を選択します。
④「出力インタフェース」は「WAN」を選択します。
⑤「送信元IPアドレス／マスク長」は「指定」を選択し、「192.168.1.4／32」を入力します。
⑥「送信先IPアドレス／マスク長」は「全て」を選択します。
⑦「送信先ポート番号」は「指定」を選択し、20～21を入力します。
⑧「追加」をクリックしてください。一覧に設定したデータが追加されます。
　インターネット接続を規制する2台目のパソコンの設定も①～⑧の手順を同様に行ってください。ただし、⑤で指定する「送信元IPアドレス／マスク長」は「192.168.1.5／32」を指定します。

⑨「確認」をクリックしてください。
⑩「送信」をクリックしてください。
⑪「反映」をクリックしてください。

スタティックルーティングをするには

ルーティングテーブルをあらかじめ本商品に設定しておくことで、常に固定的なルートを選択すること(スタティックルーティング)ができます。ルーティングテーブルには経路毎に宛先ネットワークアドレス/マスク長とゲートウェイアドレスの組み合わせを指定します。ここでは以下のように本商品にローカルルータ（ルータ A）が設置されていることを前提にローカルルータ配下に接続されたパソコン宛てのパケットを本商品からローカルルータに転送するようなルーティングテーブルの設定手順について説明します。

こんなときにはこの設定

Webブラウザで本商品にログインし、メニューの「ルータ設定」－「ルーティング条件（メインセッション)」をクリックします。

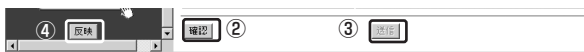
①宛先ネットワークアドレスは「192.168.10.0／24 」を入力します。
②「ゲートウェイアドレス」は「192.168.1.3」を入力します。
③「追加」をクリックしてください。一覧に設定したデータが追加されます。

④「確認」をクリックしてください。
⑤「送信」をクリックしてください。
⑥「反映」をクリックしてください。

IPv6フレームをブリッジするには

IPv6フレームをブリッジすることができます。 IPv6サービスを利用するときには、以下のようにIPv6 ブリッジ機能を「有効」に設定します。

Webブラウザで本商品にログインし、メニューの「ルータ設定」－「ネットワーク設定」をクリックします。

①「IPv6ブリッジ設定」は「有効」を選択します。

②「確認」をクリックしてください。
③「送信」をクリックしてください。
④「反映」をクリックしてください。

お知らせ

- 「動作モード」が「PPPoE」のときにのみ、IPv6ブリッジが動作します。（「ネットワーク設定」（☛P2-8））
- IPv6サービス（「IPv6ブリッジ設定」＝「有効」）とIEEE802.11bおよびIEEE802.11g（「無線動作モード」＝「11b+g」）を同時に利用すると、無線LANクライアント側のパソコンでインターネットに接続できなかったり、通信が切れる場合があります。（「ネットワーク設定」（☛P2-8））

こんなときにはこの設定

特定の相手からの呼び出しを拒否するには

Webブラウザまたは電話機から本商品に設定を行うことで着信を拒否したい相手先電話番号を本商品に登録することができます。

■Webブラウザからの設定方法

「サービス設定」（☛P2-43）を参照してください。

■電話機からの設定方法

「機能仕様」の「着信拒否」（☛P5-3）を参照してください。

お知らせ

●加入電話回線経由の呼び出しを拒否する場合は、当社のサービス「迷惑電話おことわりサービス」（有料）をご契約ください。

LAN側に接続したパソコンのファイルやプリンタを共有するには

本商品の設定変更は不要です。お使いのパソコンやプリンタの取扱説明書に従って設定を行ってください。

2 詳細設定方法

この章では、Webブラウザによる各設定の使い方について説明しています。

Webブラウザによる設定について・・・・2-2

Webブラウザによる設定について

本商品のデータ変更や状態確認はWebブラウザにて実施します。Webブラウザは、取扱説明書「かんたん設定」の手順を実施することにより表示されます。

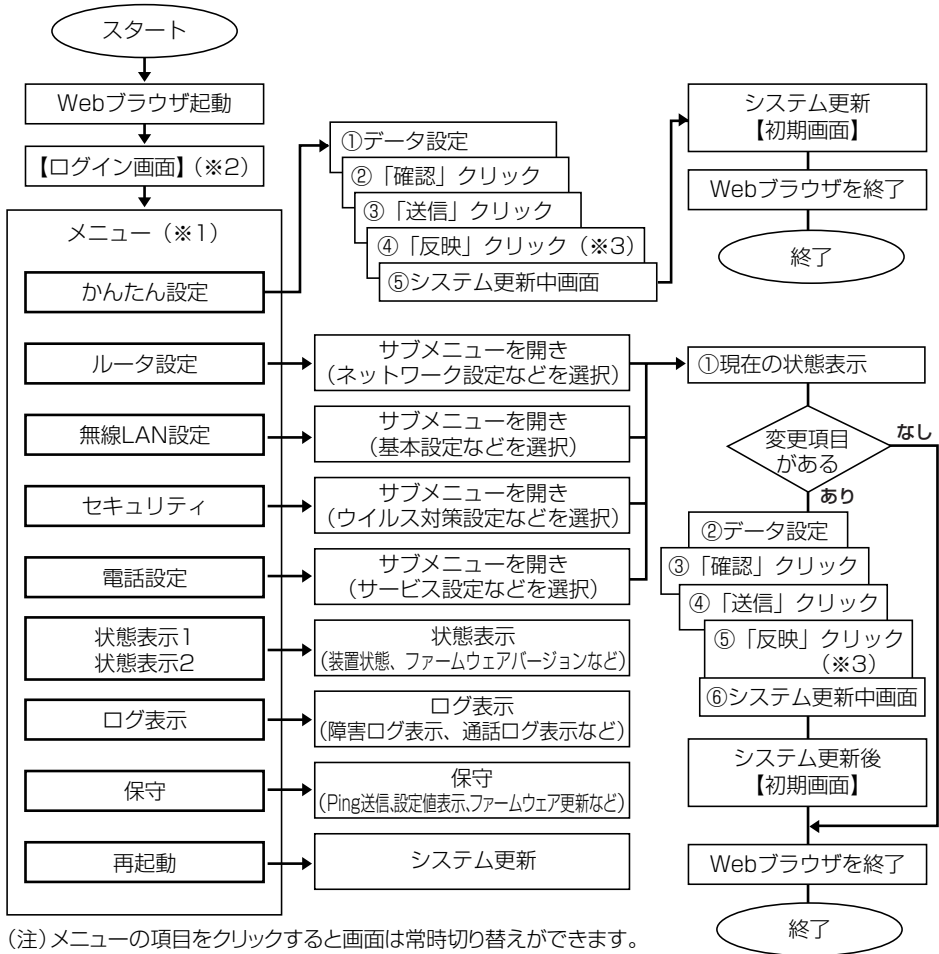
機能

機能は大きく分けると次のようになっています。

メニュー項目	機　能
かんたん設定	本商品を接続してご利用開始までに最低限必要なデータ設定を行います。
ルータ設定	本商品のルータ機能の設定変更を行う場合に利用します。
無線LAN設定	本商品の無線機能の設定変更を行う場合に利用します。
セキュリティ	本商品のセキュリティ機能の設定変更を行う場合に利用します。
電話設定	IP電話サービスや加入電話サービス等の電話サービスに関する設定変更を行う場合に利用します。
状態表示1 状態表示2	本商品の運用状態を確認する場合に利用します。また、ファームウェア手動アップデートやPPPoEの手動接続/切断を実施することができます。
ログ表示	本商品の履歴情報を確認する場合に利用します。
保守	通信試験や最新バージョンへのバージョンアップを実施する場合に利用します。
再起動	システム更新や、初期設定状態に戻す際に利用します。

操作の流れ

操作の基本的な流れを示します。

（注）メニューの項目をクリックすると画面は常時切り替えができます。

※1　画面左にメニューが表示されます。項目をクリックすると画面が切り替わります。
※2　初期状態のときは、ログイン後に最新ファームウェアの確認とバージョンアップを行います。（取扱説明書「かんたん設定」）
※3　全てのデータを設定後に実施します。（サブメニュー単位に実施する必要はありません。「確認」「送信」クリックはサブメニュー単位に実施してください。）システム更新後、設定したデータが反映されます。

Webブラウザによる設定について

ボタンについて

Webブラウザ上で使用するボタンについて説明します。

● 「確認」ボタン
Webブラウザ上で設定した内容を確認します。変更した内容が不正なときはポップアップメッセージが表示されます。正しい内容を再入力し、もう一度「確認」をクリックしてください。

● 「送信」ボタン
Webブラウザ上で設定した内容を本商品へ送信します。
「確認」をクリックし、正しい内容が入力されている場合に「送信」は有効になります。

● 「反映」ボタン
「送信」をクリックし、送信した内容を設定します。その後「反映」をクリックするとシステム更新を実施しWebブラウザで設定した内容で起動します。

ご利用方法

Webブラウザのご利用方法および、各メニューの詳細内容について説明します。
画面構成は下表のとおりです。

メニュー	サブメニュー	参照
かんたん設定	ー	「かんたん設定」
ルータ設定	ネットワーク設定	「ネットワーク設定」（☛P2-8）
	PPPoE設定	「PPPoE設定」（☛P2-11）
	DHCP設定	「DHCP設定」（☛P2-14）
	NAPT設定	「NAPT設定」（☛P2-17）
	IPフィルタ設定	「IPフィルタ設定」（☛P2-20）
	ルーティングテーブル設定	「ルーティングテーブル設定」（☛P2-22、P2-24）
	ルーティング条件（メインセッション）	「ルーティング条件（メインセッション）」（☛P2-22）
	ルーティング条件（サブセッション）	「ルーティング条件（サブセッション）」（☛P2-24）
	RIP設定	「RIP設定」（☛P2-27）
	VPNパススルー設定	「VPNパススルー設定」（☛P2-28）
	SPI設定	「SPI設定」（☛P2-30）
	Dynamic DNS設定	「Dynamic DNS設定」（☛P2-32）
	Windows共有フィルタ/ステルス設定	「Windows共有フィルタ/ステルス設定」（☛P2-34）
無線LAN設定	基本設定	「基本設定」（☛P2-36）
	暗号化設定	「暗号化設定」（☛P2-36）
	MACアドレスフィルタリング	「MACアドレスフィルタリング」（☛P2-37）
セキュリティ	ウイルス対策設定	「ウイルス対策設定」（☛P2-40）
	アップデート設定	「アップデート設定」（☛P2-41）
電話設定	サービス設定	「サービス設定」（☛P2-43）
	IP電話設定情報	「IP電話設定情報」（☛P2-46）
状態表示1	ー	「状態表示1」（☛P2-48）
状態表示2	ー	「状態表示2」（☛P2-51）
ログ表示	障害ログ表示	「障害ログ表示」（☛P2-58）
	通話ログ表示	「通話ログ表示」（☛P2-58）
	不正アクセスログ表示	「不正アクセスログ表示」（☛P2-59）
	ウイルスログ表示	「ウイルスログ表示」（☛P2-59）
	アップデートログ表示	「アップデートログ表示」（☛P2-60）

（次ページに続く）

メニュー	サブメニュー	参　照
保守	パスワード設定	「パスワード設定」（☛P2-62）
	Ping送信	「Ping送信」（☛P2-63）
	設定値表示	「設定値表示」（☛P2-63）
	ファームウェア更新	「ファームウェア更新」（☛P2-63）
	自動アップデート	「自動アップデート」（☛P2-63）
再起動	―	「再起動」（☛P2-64）

かんたん設定（オンライン登録含む）

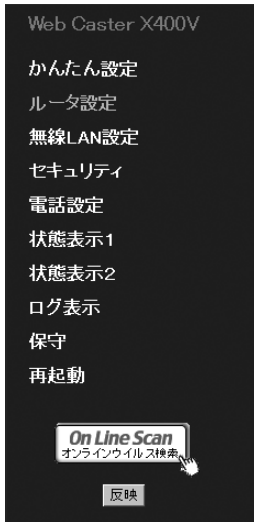
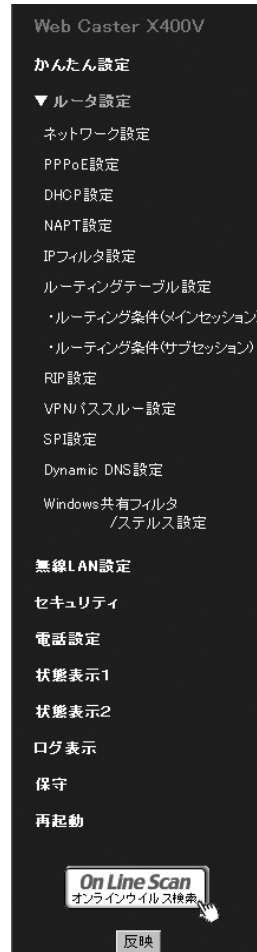
- 「かんたん設定」の設定の仕方は取扱説明書「かんたん設定」を参照し、設定は必ず行ってください。
- 「オンライン登録」の仕方は、取扱説明書「フレッツ・セーフティ登録と廃止」を参照してください。

ルータ設定

本商品の設定を変更することができます。

1 画面左メニューの「ルータ設定」をクリックします。

2 サブメニューが表示されたら、変更したい項目をクリックします。

Webブラウザによる設定について

■ネットワーク設定

LAN側およびWAN側のネットワークに関するデータを変更することができます。

1 サブメニューの「ネットワーク設定」をクリックすると、現在のデータ内容が画面に表示されます。

2 各項目を設定します。

項　目	内　容	初期値
<動作モード>		
動作モード	ネットワークへ接続する際の接続方法を設定します。 設定範囲 ：PPPoE/DHCP/固定IP PPPoE ：本商品のPPPoEクライアント機能により、外部PPPoE認証サーバとセッションを確立してネットワークへ接続します。PPPoEマルチセッション対応です。 DHCP ：本商品のDHCPクライアント機能により、外部DHCPサーバよりIPアドレス取得してネットワークへ接続します。 固定IP ：本商品のWAN側ネットワーク設定に固定値を指定してネットワークへ接続します。ただし、フレッツ・ADSL、Bフレッツ接続を利用してプロバイダから固定IPアドレスを割り当てられる場合には「PPPoE」を設定してください。	PPPoE

お知らせ

●「動作モード」で「DHCP」または「固定IP」に設定したときは、セキュリティ対策ファイル（検索エンジン、ファイアウォールルール、ウイルスパターン）のバージョンアップができません。
●「動作モード」を「DHCP」または「固定IP」から「PPPoE」に変更したとき、ファームウェアの自動バージョンアップが行われる場合があります。

項　目	内　容	初期値
<WAN側ネットワーク設定>		
WAN側IPアドレス/マスク長	動作モードが「固定IP」を選択した場合に使用する設定項目です。本設定は固定的に割り当てられたIPアドレスおよびサブネットマスクを使用してネットワークに接続する場合に設定します。 ・ WAN側IPアドレス：WAN側ネットワークに割り当てられたIPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255 ・ マスク長：WAN側ネットワークに割り当てられたサブネットマスクを設定します。 設定範囲：1～32	なし/なし
デフォルトゲートウェイ	動作モードが「固定IP」を選択した場合に使用する設定項目です。本設定はWAN側ネットワークに割り当てられたデフォルトゲートウェイを設定します。	なし
<DNSリレー設定>		
DNSサーバアドレス	DNSサーバのIPアドレスを設定します。通常使用するサーバ（プライマリ）とプライマリサーバがダウンしたときに使用するサーバ（セカンダリ）のIPアドレスを設定します。プロバイダが指定した情報を使用して下さい。 設定範囲：0.0.0.1～255.255.255.255 (注) 動作モードがPPPoEで使用する場合は、PPPoE設定メニューで設定してください。	なし/なし
<NTPサーバ設定>		
NTPサーバIPアドレス	NTPサーバのアドレスを設定します。時計情報を設定する場合に使用します。プロバイダが指定した情報を使用して下さい。（取扱説明書「時刻の設定について」） 設定範囲：0.0.0.1～255.255.255.255	なし
<LAN側ネットワーク設定>		
LAN側IPアドレス/マスク長	・ LAN側IPアドレス：LAN側の IPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255 ・ マスク長：LAN側のサブネットマスクを設定します。 設定範囲：1～32	192.168.1.1/24
<IPv6ブリッジ設定>		
IPv6ブリッジ設定	IPv6サービスを利用するときは「有効」にしてください。 動作モードが「PPPoE」の場合に有効です。 設定範囲：無効/有効	無効
<ポート設定>		
WANポート設定	WAN側ポートの通信速度、モードを設定します。 通常は「自動認識」をご利用ください。 設定範囲： ・自動認識：ネゴシエーションを行い、自動で設定します。 ・100M全二重：100Mbpsの全二重通信 ・100M半二重：100Mbpsの半二重通信 ・10M全二重：10Mbpsの全二重通信 ・10M半二重：10Mbpsの半二重通信	自動認識
LAN 1ポート設定	LAN側ポート(1/2/3/4チャネル目)の通信速度、モードを設定します。通常は「自動認識」をご利用ください。 設定範囲： ・自動認識：ネゴシエーションを行い、自動で設定します。 ・100M全二重：100Mbpsの全二重通信 ・100M半二重：100Mbpsの半二重通信 ・10M全二重：10Mbpsの全二重通信 ・10M半二重：10Mbpsの半二重通信	自動認識
LAN 2ポート設定		
LAN 3ポート設定		
LAN 4ポート設定		

（次ページに続く）

Webブラウザによる設定について

3 設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

お知らせ

「IPv6ブリッジ」について
- IPv6の通信については、本商品のセキュリティ機能はご利用になれませんのでご注意ください。
- IPv6サービス（「IPv6ブリッジ設定」＝「有効」）とIEEE802.11bおよびIEEE802.11g（「無線動作モード」＝「11b+g」）を同時に利用すると、無線LANクライアント側のパソコンでインターネットに接続できなかったり、通信が切れる場合があります。

ワンポイント

- 【参考】NTPサーバの初期設定状態は、インターネットマルチフィード株式会社の“時刻提供サービスfor Pulic”を利用しています。
  免責事項等については以下URLをご覧ください。
  http://www.jst.mfeed.ad.jp/

■PPPoE設定

PPPoEに関するデータを変更することができます。

(注1)「ネットワーク設定：動作モード」で「PPPoE」を選択した場合に利用します。
(注2)「接続先1～4」で使用するアカウントを設定することができます。

1 サブメニューの「PPPoE設定」をクリックすると、現在のデータ内容が表示されます。

(次ページに続く)

Webブラウザによる設定について

2 各項目を設定します。

項　目	内　容	初期値
セッション設定		
契約セッション数	契約したセッション数を設定します。 設定範囲：2～5	2
メインセッション	メインセッションを選択します。 「使用するセッション」に選択されている中からメインセッションを選択してください。 ※ここで選択したセッションがIP電話で使用するセッションになります。	なし
使用するセッション	使用する接続先を選択してください。使用するセッションが、契約セッション数を超えないようにしてください。 ※接続先5で使用するセッションは変更できません。	接続先5
インターネットサービスプロバイダ設定		
接続先1～4		
接続ユーザ名	プロバイダから指定されたログインID名※を入力してください。 「動作モード」で「PPPoE」以外を設定する場合は、ここに設定する必要はありません。	なし
接続パスワード	プロバイダから指定されたログインパスワード※を入力してください。 「動作モード」で「PPPoE」以外を設定する場合は、ここに設定する必要はありません。	なし
接続パスワード確認	確認のためにもう一度同じパスワードを入力してください。	なし
認証方式	PPPoEの認証方式を設定します。PAP+CHAPを選択した場合、接続先と一致した方式を利用します。 設定範囲：認証なし/PAP/CHAP/PAP+CHAP	PAP+CHAP
無通信監視タイマ	インターネットへのアクセスが一定時間ないときに、セッションを自動的に切断します。 設定範囲：無効/1/5/10/30（分）	無効
DNSサーバアドレス	DNSサーバのIPアドレスを設定します。プロバイダから指定された場合にのみ設定してください。設定されている場合はPPPoE機能により取得したDNSサーバアドレスではなく本データを利用します。 通常使用するサーバ（プライマリ）とプライマリサーバがダウンしたときに使用するサーバ（セカンダリ）のIPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	なし
MTU値	MTU値を設定します。 設定範囲：576～1492（4の倍数を推奨） ※設定を変更すると通信できなくなることがあります。ご注意ください。	1452
IPアドレス指定	Unnumbered接続の場合、「指定する」を設定し、プロバイダから割り当てられたIPアドレス/マスク長を入力します。（「複数の固定IPアドレス（Unnumbered）サービスを利用するには」（☛P1-12）） 設定範囲：指定しない/指定する （IPアドレス）0.0.0.1～255.255.255.255 （マスク長）1～32	指定しない

※プロバイダによってログインID名、ログインパスワードの呼び方が異なります。

項　目	内　容	初期値
接続先5：フレッツ・スクウェア接続設定		
接続ユーザ名	初期設定画面のフレッツ・スクウェア設定の「エリア選択」にて決定されます。 入力による変更はできません。	NTT東日本： guest@flets NTT西日本： flets@flets
接続パスワード	初期設定画面のフレッツ・スクウェア設定の「エリア選択」にて決定されます。 入力による変更はできません。	NTT東日本：guest NTT西日本：flets
接続パスワード確認	初期設定画面のフレッツ・スクウェア設定の「エリア選択」にて決定されます。 入力による変更はできません。	NTT東日本：guest NTT西日本：flets
無通信監視タイマ	フレッツ・スクウェアへのアクセスが一定時間ないときに、セッションを自動的に切断します。デフォルトで1（分）の無通信監視タイマが設定されています。 設定範囲：1/5/10/30（分）	1

3 設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

お知らせ

- Unnumbered接続時には、セキュリティ機能の一部がご利用できない場合があります。（取扱説明書「セキュリティに関するご注意」）
- お客様の契約数以上のセッション数を設定した場合は、フレッツ・セーフティの機能がご利用できなくなります。

■DHCP設定

DHCPサーバに関するデータを変更することができます。
※「ネットワーク設定：動作モード」に関係なく設定することができます。

1 サブメニューの「DHCP設定」をクリックすると、現在のデータ内容が表示されます。

2 各項目を設定します。

項　目	内　容	初期値
<LAN側ネットワーク設定>		
LAN側IPアドレス/マスク長	・LAN側IPアドレス： LAN側の IPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255 ・マスク長：LAN側のサブネットマスクを設定します。 設定範囲：1～32 ※「ネットワーク設定」のLAN側IPアドレス/マスク長の内容が反映されます。	192.168.1.1/24
<DHCPサーバ設定>		
DHCPサーバ機能	DHCPサーバとして動作させるときは有効を設定します。 プルダウンメニューから有効/無効を設定してください。	有効
割り当て開始IPアドレス	本商品の「DHCPサーバ機能」を「有効」にしたとき、DHCPサーバから割り当てるIPアドレスの割り当て開始IPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255 （注）IPアドレス割り当て範囲は、LAN側IPアドレスと同一のサブネットでLAN側IPアドレスが含まれない範囲を指定してください。	192.168.1.2
割り当て終了IPアドレス	本商品の「DHCPサーバ機能」を「有効」にしたとき、DHCPサーバから割り当てるIPアドレスの割り当て終了IPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	192.168.1.11
DNSサーバアドレス	本商品の「DHCPサーバ機能」を「有効」にしたとき、DHCPサーバから割り当てる範囲のIPアドレスをDNSサーバアドレスに設定することができます。設定値は本商品のLAN側のIPアドレスを推奨します。 設定範囲：0.0.0.1～255.255.255.255 （注）本商品のLAN側IPアドレスを推奨します。	192.168.1.1

3 固定IPアドレスで使用する端末の情報設定をします。

(1) 固定IPアドレスで使用する端末の情報設定

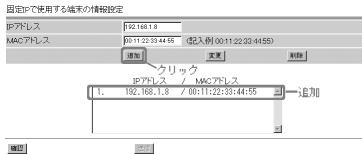
特定の装置に固定的にIPアドレスを割り当てることを可能とするため、MACアドレスとIPアドレスの組み合わせを設定します。

設定範囲：1～16パターン

(2) 追加方法

①各項目を設定します。

項　目	内　容	初期値
IPアドレス	IPアドレスを固定して使用したいときに設定します。固定IPアドレスの設定はLAN側IPアドレス/マスク長の範囲を推奨します。 設定範囲：0.0.0.1～255.255.255.255	なし
MACアドレス	DHCPで固定のIPアドレスを割り当てるパソコンのMACアドレスを半角数字で設定します。MACアドレスは「ipconfig」などのネットワーク状況を確認するコマンドを投入した時に「Physical Address」として表示されます。 （記入例：00:11:22:33:AA:BB）	なし

②「追加」をクリックしてください。次のように一覧に追加されます。

内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法

①変更するデータを選択し、データを変更します。

②「変更」をクリックしてください。一覧が更新されます。

内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

4 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

（次ページに続く）

Webブラウザによる設定について

5 「送信」をクリックします。

6 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

■NAPT設定

NAPTに関するデータを変更することができます。

1 サブメニューの「NAPT設定」をクリックすると現在のデータ内容が表示されます。

2 各項目を設定します。

項　目	内　容	初期値
動的NAPT機能	動的NAPT機能の無効/有効を設定します。 設定範囲：無効 / 有効	有効
簡易DMZ IPアドレス	グローバル側（WAN側）からのアクセスを特定の端末へ転送する機能です。LAN側転送先のIPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	なし
<UPnP設定>		
UPnP機能	接続先1 有効～接続先5 有効/無効を選択してください。 ※UPnP機能はいずれかの接続先しか「有効」にすることができません。	無効

お知らせ

- ●動的NAPT機能を無効に設定すると、セキュリティ機能の一部がご使用できない場合があります。
- ●UPnP機能を有効に設定すると、セキュリティ機能の一部がご使用できない場合があります。
- ●「簡易DMZ IPアドレス」機能を利用してLAN側のIPアドレスを設定すると、セキュリティ機能の一部が利用できない場合があります。（取扱説明書「セキュリティに関するご注意」）

（次ページに続く）

Webブラウザによる設定について

3 静的NAPT設定（ポート転送規則）をします。

(1) 静的NAPT機能で使用するポート転送規則の設定
LAN側の端末がインターネット上の端末にアクセスする場合、LAN側転送IPアドレス/転送ポート番号とWAN側ポート番号の組み合わせを設定します。
設定範囲：1〜32パターン

(2) 追加方法
①各項目を設定します。

項　目	内　容	初期値
割り当てWAN側受信ポート範囲	転送させたいWAN側受信ポート範囲を設定します。 設定範囲：1〜65535 ※ポートの範囲は16以内にしてください。（例：1001〜1016）	なし
プロトコル種別	使用するプロトコルを設定します。 設定範囲：TCP / UDP	なし
LAN側転送IPアドレス	LAN側転送先のIPアドレスを設定します。 設定範囲：0.0.0.1〜255.255.255.255	なし
LAN側転送ポート	LAN側転送先ポート番号を指定してください。 設定範囲：1〜65535 （例）割り当てWAN側受信ポート範囲を1001〜1003、転送先ポートを1001にした場合は以下のように転送されます。 ・ポート1001で受信→1001へ転送 ・ポート1002で受信→1002へ転送 ・ポート1003で受信→1003へ転送	なし

②「追加」をクリックしてください。次のように一覧に追加されます。
内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法
①変更するデータを選択し、データを変更します。
②「変更」をクリックしてください。一覧が更新されます。
内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法
①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

4 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

5 「送信」をクリックします。

6 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

ワンポイント

お客さまがネットワーク対応アプリケーション（ネットワークゲームなど）を使用する場合、ゲームのWebサイトの環境によっては本商品の静的NAPT設定（ポート転送規則）の「割り当てWAN側受信ポート範囲」は最大16ポートの制限を超える場合があります。この場合は、以下のように設定することでご使用できます。

設定例）ネットワークゲームを行うLAN側のパソコンのIPアドレスが192.168.1.10の例において、Webサイトのネットワークゲームで使用するポートの範囲が以下の場合
使用しているポート
・TCP 2300-2331
・UDP 2300-2331

登録データ例）
以下のように複数登録して使用します。

エントリ1：割り当てWAN側受信ポート範囲：2300-2315
プロトコル種別：TCP
LAN側転送IPアドレス：192.168.1.10
LAN側転送ポート：2300

エントリ2：割り当てWAN側受信ポート範囲：2316-2331
プロトコル種別：TCP
LAN側転送IPアドレス：192.168.1.10
LAN側転送ポート：2316

エントリ3：割り当てWAN側受信ポート範囲：2300-2315
プロトコル種別：UDP
LAN側転送IPアドレス：192.168.1.10
LAN側転送ポート：2300

エントリ4：割り当てWAN側受信ポート範囲：2316-2331
プロトコル種別：UDP
LAN側転送IPアドレス：192.168.1.10
LAN側転送ポート：2316

■ IPフィルタ設定

IPパケットフィルタリングに関するデータを変更することができます。

1 サブメニューの「IPフィルタ設定」をクリックすると、現在のデータ内容が表示されます。

2 デフォルトの規則を設定します。

項　目	内　容	初期値
デフォルトの規則	<パケットフィルタ規則>で指定しないIPアドレス・ポート番号からのアクセスを許可する/破棄するを指定します。	許可

3 パケットフィルタ規則の設定をします。

(1) パケットフィルタ規則の設定
　パケットフィルタリングを実施するため、パケットフィルタ規則を設定します。
　設定範囲：１～64パターン

(2) 追加方法
　①各項目を設定します。

項　目	内　容	初期値
方針（POLICY）	許可/破棄から選択します。	なし
プロトコル種別 (PROTOCOL)	全て/TCP/UDP/ICMPから選択します。	なし
入力インタフェース（IN）	全て/WAN/LAN/接続先を1つ選択（接続先1～5）から選択します。	なし
出力インタフェース（OUT）	全て/WAN/LAN/接続先を1つ選択（接続先1～5）から選択します。	なし
送信元IPアドレス/マスク長 (SOURCE IP/ MASK)	全て/指定（IPアドレス/マスク長） IPアドレスの設定範囲：0.0.0.1～255.255.255.255 マスク長の設定範囲：1～32	なし/なし
送信先IPアドレス/マスク長 (DESTINATION IP/ MASK)	全て/指定（IPアドレス/マスク長） IPアドレスの設定範囲：0.0.0.1～255.255.255.255 マスク長の設定範囲：1～32	なし/なし
送信先ポート番号（PORT）	全て/指定（範囲指定） ポート番号の設定範囲：1～65535	なし

②「追加」をクリックしてください。次のように一覧に追加されます。「接続先1～接続先5」は、一覧では「S1～S5」と表示されます。
内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法

①変更するデータを選択し、データを変更します。

②「変更」をクリックしてください。一覧が更新されます。
内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

4 **すべての設定が終了したら「確認」をクリックします。**

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

5 **「送信」をクリックします。**

6 **「反映」をクリックします。**

システム更新終了後、設定した内容が有効になります。

お知らせ

●ウイルス検索の対象が使用するポート（25（メール送受信：SMTP）、80（Web：HTTP）、110（メール受信：POP3））についてはIPアドレス／ポートフィルタ機能はご利用できません。

Webブラウザによる設定について

■ ルーティングテーブル設定　ルーティング条件（メインセッション）

「PPPoE設定」画面の「セッション設定」で設定した「メインセッション」のルーティング条件を設定します。IPパケットを送出する時の経路表を固定的に設定できます。

1 サブメニューの「ルーティング条件（メインセッション）」をクリックすると現在のデータ内容が画面に表示されます。

（1）スタティックルーティングの設定
　IPパケットが宛先ネットワークアドレスに届くまでの経路情報を設定します。
　設定範囲：0〜16パターン
（2）追加方法
　①各項目を設定します。

項　目	内　容	初期値
<スタティックルーティング設定>		
宛先ネットワークアドレス / マスク長	・宛先ネットワークアドレス： 宛先ネットワークのIPアドレスを設定します。 設定範囲：0.0.0.1〜255.255.255.255 ・マスク長：サブネットマスク値を設定します。 設定範囲：1〜32 ※設定例 宛先ネットワークアドレス：100.100.100.1 マスク長：24 のような設定はできません。 ⇒宛先ネットワークアドレス：100.100.100.0 のようにマスク長を考慮して設定してください。	なし
ゲートウェイIPアドレス	ゲートウェイIPアドレスを設定します。 設定範囲：0.0.0.1〜255.255.255.255	なし

　②「追加」をクリックしてください。次のように一覧に追加されます。
　　内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法

①変更するデータを選択し、データを変更します。

②「変更」をクリックしてください。一覧が更新されます。
内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

2 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

3 「送信」をクリックします。

4 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

Webブラウザによる設定について

■ ルーティングテーブル設定　ルーティング条件（サブセッション）

サブセッションのルーティング条件はフレッツ・スクウェア用のルーティング設定が固定で入力されておりますが、ルーティング条件の追加をすることは可能です。追加する場合には以下の手順で設定してください。IPパケットを送出する時の経路表を固定的に設定できます。

1 サブメニューの「ルーティング条件（サブセッション）」をクリックすると現在のデータ内容が画面に表示されます。

追加するドメイン名

(1) 追加するドメイン名の設定
　追加するドメインを設定します。追加方法は以下のとおりです。
　設定範囲：2～16パターン。1パターンは固定です。

(2) 追加方法
　①各項目を設定します。

項　目	内　容	初期値
追加するドメイン名	設定範囲：英数字（0～9)、大文字/小文字アルファベット（a～z、A～Z）およびハイフン(-)、ピリオド(.)（1～最大63文字） ※先頭と最後は半角英数字を入力してください。 （先頭のピリオドは入力する必要はありません。） 設定例）flets ○　.flets ×（先頭がピリオド（.）のため） 接続先：「接続先1」～「接続先5」から選択してください。	パターン1=flets

　②「追加」をクリックしてください。下図のように一覧に追加されます。「接続先1～接続先5」は、一覧では「S1～S5」と表示されます。
　内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

（注）「flets」のルール（パターン1）は削除できません。

(3) 変更方法
　①変更するデータを選択し、データを変更します。
　②「変更」をクリックしてください。一覧が更新されます。
　内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

追加する宛先ネットワークアドレス/マスク長

(1) 追加する宛先ネットワークアドレス/マスク長の設定

追加する宛先ネットワークアドレス/マスク長を設定します。追加方法は以下のとおりです。
設定範囲：1～16パターン

(2) 追加方法

①各項目を設定します。

項　目	内　容	初期値
追加する宛先ネットワークアドレス/マスク長	追加する宛先ネットワークアドレス： 宛先ネットワークのIPアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255 マスク長：サブネットマスク値を設定します。 設定範囲：1～32 接続先：「接続先1」～「接続先5」から選択してください。 ※ドメインとネットワークアドレスの両方を設定された場合はドメインのデータが優先されます。 ※設定例 宛先ネットワークアドレス：100.100.100.1 マスク長：24 のような設定はできません。 ⇒宛先ネットワークアドレス：100.100.100.0 のようにマスク長を考慮して設定してください。	なし

②「追加」をクリックしてください。下図のように一覧に追加されます。「接続先1～接続先5」は、一覧では「S1～S5」と表示されます。
内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法

①変更するデータを選択し、データを変更します。

②「変更」をクリックしてください。一覧が更新されます。
内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

①削除するデータを選択し「削除」をクリックしてください。一覧から選択したデータが削除されます。

（次ページに続く）

Webブラウザによる設定について

2 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

3 「送信」をクリックします。

4 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

■ RIP設定

RIP設定に関するデータを変更することができます。

1 サブメニューの「RIP設定」をクリックすると現在のデータ内容が表示されます。

2 各項目を設定します。

項　目	内　容	初期値
<各インタフェースのRIP設定>		
LANインタフェース	LAN側インタフェースのRIPの有効／無効を選択してください。	無効
WANインタフェース	WAN側インタフェースのRIPの有効／無効を選択してください。「有効」としたときは対象となる接続先を選択してください。	無効

3 設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

ワンポイント

● RIPのバージョン1に対応します。（クラスレスアドレスはご利用になれません。）

■ VPNパススルー設定

VPNパススルーに関するデータを変更することができます。本商品は、LAN側から発生するVPN通信の監視を行い、その通信の情報を元にWAN側からの通信を自動的にLAN側へ転送します。このため、LAN側から通信を開始する場合、VPNパススルーの設定を行う必要はありません。WAN側から通信を開始したい場合に、本設定を行ってください。

1 現在のPPTP、IPsec、L2TP各パススルー設定状態を表示します。サブメニューの「VPNパススルー設定」をクリックすると現在のデータ内容が表示されます。

2 現在の各パススルー設定に変更を入れる場合には各項目を設定します。

項　目	内　容	初期値
<PPTPパススルー設定（サーバ公開）>		
WANからLANへのアクセス	WAN側からLAN側へPPTPパススルーによるアクセスを許可するかどうかを設定します。 設定範囲：無効/有効	無効
LAN側IPアドレス	アクセスを許可するLAN側のホストアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	なし
WAN側IPアドレス	アクセスを許可するWAN側のホストアドレスを設定します。 設定範囲：すべて/指定 WAN側IPアドレス指定時の設定範囲： 0.0.0.1～255.255.255.255	すべて
<IPsecパススルー設定（サーバ公開）>		
WANからLANへのアクセス	WAN側からLAN側へIPsecパススルーによるアクセスを許可するかどうかを設定します。 設定範囲：無効/有効	無効
LAN側IPアドレス	アクセスを許可するLAN側のホストアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	なし
WAN側IPアドレス	アクセスを許可するWAN側のホストアドレスを設定します。 設定範囲：すべて/指定 WAN側IPアドレス指定時の設定範囲： 0.0.0.1～255.255.255.255	すべて

項　目	内　容	初期値
<L2TPパススルー設定（サーバ公開）>		
WANからLANへのアクセス	WAN側からLAN側へL2TPパススルーによるアクセスを許可するかどうかを設定します。 設定範囲：無効/有効	無効
LAN側IPアドレス	アクセスを許可するLAN側のホストアドレスを設定します。 設定範囲：0.0.0.1～255.255.255.255	なし
WAN側IPアドレス	アクセスを許可するWAN側のホストアドレスを設定します。 設定範囲：すべて/指定 WAN側IPアドレス指定時の設定範囲： 0.0.0.1～255.255.255.255	すべて

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

お知らせ

●VPNをご使用する端末に対しては、セキュリティ機能の一部がご使用できない場合があります。

■SPI（ステートフルパケットインスペクション）設定

SPI（ステートフルパケットインスペクション）に関するデータを変更することができます。本設定では、本商品を通過するパケットのデータの状態により動的にポートを開放、閉鎖し、LAN側のネットワークを不正アクセスから保護します。

1 現在のSPI設定状態を表示します。サブメニューの「SPI（ステートフルパケットインスペクション）設定」をクリックすると現在のデータ内容が表示されます。

2 現在の各SPI設定に変更を入れる場合は各項目を設定します。

項　目	内　容	初期値
〈タイムアウト設定〉		
ICMP	ICMPパケットのアイドル時間（単位は秒）のタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	30
UDPアイドル	UDPアイドルパケットのアイドル時間（単位は秒）のタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	30
UDP STREAM	UDP STREAMパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	180
TCP ESTABLISHED	TCP ESTABLISHEDパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	432000
TCP SYNSENT	TCP SYNSENTパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	120
TCP SYNRECV	TCP SYNRECVパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	60

項　目	内　容	初期値
TCP FINWAIT	TCP FINWAITのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	120
TCP TIMEWAIT	TCP TIMEWAITパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	120
TCP CLOSE	TCP CLOSEパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	10
TCP CLOSEWAIT	TCP CLOSEWAITパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	60
TCP LASTACK	TCP LASTACKパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	30
TCP LISTEN	TCP LISTENパケットのタイムアウト時間を設定します。タイムアウト時間を過ぎると本通信セッションは遮断されます。 設定範囲：1～1209600秒（最大2週間）	120
＜TCPセッション制限＞		
セッション数	本商品を通過することができるTCPセッション数の最大値を設定します。 設定例）WebブラウザでHTTPプロトコルによるTCPセッションの最大接続数を30にしたい場合は下記の値を設定します。 セッション数：30 TCPポート番号：80 設定範囲：1～255	なし
TCPポート番号	TCPセッション数の制限を行うTCPポート番号を設定します。ALLの場合は全TCPセッション数を制限します。 設定範囲：ALL/ポート番号指定 ポート番号の設定範囲：1～65535	なし

※TCPセッション制限は最大16個まで登録できます。

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

Webブラウザによる設定について

■Dynamic DNS設定

Dynamic DNSに関する設定を変更することができます。

1 現在のDynamic DNS設定状態を表示します。サブメニューの「Dynamic DNS設定」をクリックすると現在のデータ内容が表示されます。

2 現在のDynamic DNS設定に変更を入れる場合は各項目を設定します。

項　目	内　容	初期値
<Dynamic DNS設定>		
Dynamic DNS設定	Dynamic DNS機能の有効/無効を設定します。 設定範囲：有効/無効	無効
認証方法	Dynamic DNS機能を有効にしたとき認証方法を設定します。 設定範囲：なし/BASIC認証	なし
認証ID	Dynamic DNS機能を有効にしたとき認証IDを設定します。	なし
認証パスワード	Dynamic DNS機能を有効にしたとき認証IDに対する認証パスワードを設定します。	なし
更新タイマ	Dynamic DNS機能を有効にしたとき更新時間を設定します。 設定範囲：1～24（時間）	2
<Dynamic DNS URL設定>		
登録先URL	Dynamic DNSサーバのURLを設定します。URL内でIPアドレスを指定する必要がある場合、本商品のIPアドレスを記述する部分は「_MYIPADDR_」と設定してください。	なし

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

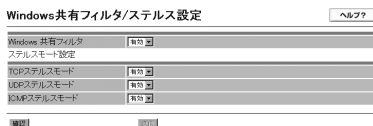
システム更新終了後、設定した内容が有効になります。

Webブラウザによる設定について

■Windows共有フィルタ/ステルス設定

外部からのアクセスに対して、本商品のセキュリティに関するデータを変更することができます。

1 サブメニューの「Windows共有フィルタ/ステルス設定」をクリックすると現在のデータ内容が表示されます。

Windows共有フィルタ/ステルス設定 ヘルプ?
Windows 共有フィルタ 有効
ステルスモード設定
TCPステルスモード 有効
UDPステルスモード 有効
ICMPステルスモード 有効
確認 送信

2 各項目を設定します。

項 目	内 容	初期値
Windows共有フィルタ	外部とのWindows共有関係（NetBIOS）のトラフィックを遮断する場合「有効」に設定します。 プルダウンメニューから有効/無効を選択してください。	有効
<ステルスモード設定>		
TCPステルスモード	TCPプロトコルにおける本商品へのアクセスに応答するかを設定します。有効にすると応答しません。 プルダウンメニューから有効/無効を選択してください。	有効
UDPステルスモード	UDPプロトコルにおける本商品へのアクセスに応答するかを設定します。有効にすると応答しません。 プルダウンメニューから有効/無効を選択してください。	有効
ICMPステルスモード	ICMPプロトコルにおける本商品へのアクセスに応答するかを設定します。有効にすると応答しません。 プルダウンメニューから有効/無効を選択してください。	有効

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

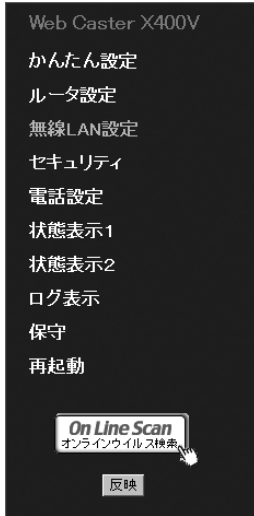
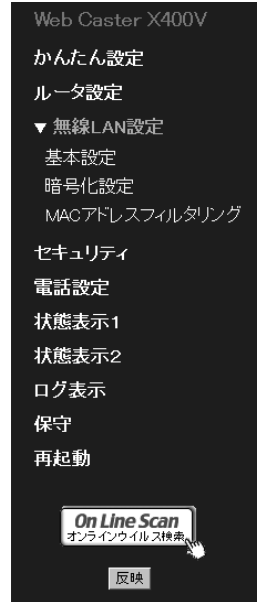
お知らせ

- セキュリティメニューの「ウイルス対策設定」の「不正アクセスレベル」を「低」にすると、「ICMPステルスモード」は「無効」に設定されます。

無線LAN設定

1 画面左メニューの「無線LAN設定」をクリックします。

2 サブメニューが表示されたら、変更したい項目をクリックします。

Webブラウザによる設定について

■基本設定

基本設定に関する設定を変更することができます。
「3 無線LANを利用する」の「④本商品の無線LAN設定を確認する」（☛P3-11）を参照してください。

■暗号化設定

暗号化設定に関する設定を変更することができます。
「3 無線LANを利用する」の「③本商品に暗号化を設定する」（☛P3-6）を参照してください。

■MACアドレスフィルタリング

MACアドレスフィルタリングに関する設定を変更することができます。無線端末のMACアドレスを登録することで、無線LANで端末以外からのアクセスを制限することができます。

1 現在のMACアドレスフィルタリングの設定状態を表示します。サブメニューの「MACアドレスフィルタリング」をクリックすると現在のデータ内容が表示されます。

2 現在の各MACアドレスフィルタリングに変更を入れる場合は各項目を設定します。

項　目	内　容	初期値
<MACアドレスフィルタリング>		
MACアドレスフィルタリング	MACアドレスフィルタリングの有効/無効を設定します。「有効」に設定した場合は「デフォルトポリシー」および「フィルタリングするMACアドレスの情報設定」の設定をします。 設定範囲：無効/有効	無効
デフォルトポリシー	デフォルトポリシーの設定をします。※1 設定範囲：拒否/許可	拒否
<フィルタリングするMACアドレスの情報設定>		
MACアドレス	MACアドレスの設定をします。最大32件登録することができます。 記入例：00:11:22:33:AA:BB	なし
ポリシー	ポリシーの設定をします。※1 設定範囲：拒否/許可	許可

※1「デフォルトポリシー」と「フィルタリングするMACアドレスの情報設定のポリシー」との関係

デフォルトポリシー	フィルタリングするMACアドレスの情報設定（ポリシー）	最終的なMACアドレスフィルタリング
拒否	登録データなし	すべてのMACアドレスからのアクセスを拒否します。
	登録データあり (拒否および許可)	許可で登録しているMACアドレスのみ許可し、その他のMACアドレスはすべて拒否します。
許可	登録データなし	すべてのMACアドレスからのアクセスを許可します。
	登録データあり (拒否および許可)	拒否で登録しているMACアドレスのみ拒否し、その他のMACアドレスはすべて許可します。

（次ページに続く）

Webブラウザによる設定について

3 **すべての設定が終了したら「確認」をクリックします。**

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 **「送信」をクリックします。**

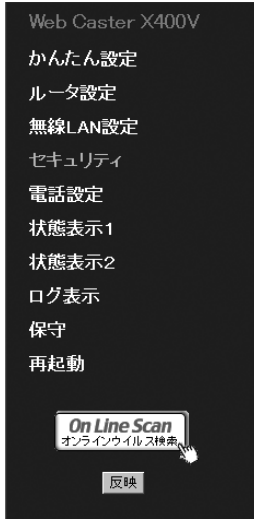
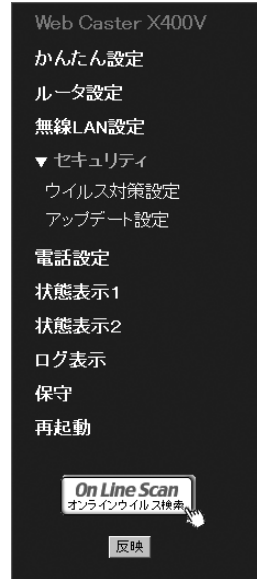
5 **「反映」をクリックします。**

システム更新終了後、設定した内容が有効になります。

セキュリティ

1 画面左メニューの「セキュリティ」をクリックします。

2 サブメニューが表示されたら、変更したい項目をクリックします。

Webブラウザによる設定について

■ウイルス対策設定

ウイルス対策設定に関する設定を変更することができます。

1 現在のウイルス対策設定の状態を表示します。サブメニューの「ウイルス対策設定」をクリックすると現在のデータ内容が表示されます。

2 現在のウイルス対策設定に変更を入れる場合は各項目を設定します。

項　目	内　容	初期値
〈不正アクセス〉		
不正アクセスレベル	必要なセキュリティレベルを選択します。 設定範囲：高/中/低 高：ハッカーの不正アクセスをブロックし、コンピュータへのアクセスが試みられたことを不正アクセスログに記録する場合は、「高」を選択します。このセキュリティレベルでは、本商品の存在は外部から見えません。したがって、ネットワークの外側からは、使用しているコンピュータやLANを見ることができません。 中：ハッカーの不正アクセスをブロックするだけの場合は、「中」を選択します。このセキュリティレベルでも、本商品の存在は外部から見えません。ハッカーの不正アクセスが検出されても不正アクセスログには記録しません。 低：必要最低限のハッカー対策機能を使用する場合は、「低」を選択します。このセキュリティレベルでは、ハッカーの不正アクセスをブロックしますが、ネットワークの外側から本商品の存在が見えます。また、ハッカーの不正アクセスが検出されても、不正アクセスログには記録されません。	高
〈ウイルス関連〉		
Eメールウイルス検索	Eメールウイルス検索をするかどうかを設定します。有効にするとウイルス検索を行います。無効にするとウイルス検索は行いません。 設定範囲：無効/有効	有効
Webメールウイルス検索	Webメールウイルス検索をするかどうかを設定します。有効にするとWebメールウイルス検索を行います。無効にするとWebメールウイルス検索は行いません。 対応しているWebメールは、Yahoo!メール、Hotmail、AOLメールです。（2005年10月現在） 設定範囲：無効/有効	有効

項　目	内　容	初期値
ウイルス検出時の処理	ウイルス検出時の処理を設定します。 設定範囲：駆除/削除/放置 ※「放置」に設定された場合でも、送信メールにウイルスが検出された場合は、削除されます。	駆除
ウイルス駆除失敗時の処理	ウイルス駆除失敗時の処理を設定します。 設定範囲：削除/放置	削除
〈通知関連〉		
e-mailアドレス	通知先のe-mailアドレスを入力します。 設定範囲：英数記号100文字	なし
e-mailアドレス確認	確認のためもう一度同じe-mailアドレスを入力してください。	なし
通知する情報	通知する情報を設定します。 ソフトウェアのアップデート：する/しない ハッカーの侵入情報：する/しない	ソフトウェアのアップデートにチェック

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

お知らせ

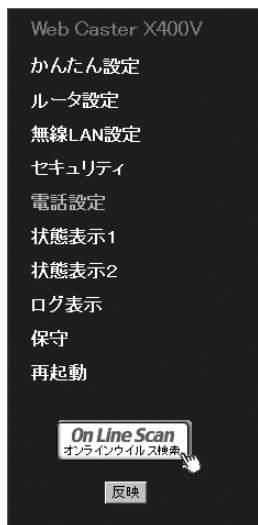
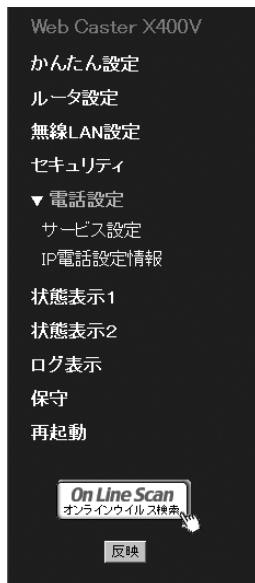
- Webブラウザ経由のウイルスチェックは非対応です。
- 「通知する情報」の「ソフトウェアアップデート」にチェックを入れている場合、フレッツ・セーフティ未登録時にはオンライン登録をご案内する内容のメールが最大5通届きます。（また、再起動すると初期化され、再度最大5通届きます。）
- ウイルス検索が有効のときはスループット最大約60Mbps（Eメールウイルス検索のみ有効設定時。Webメールウイルス検索有効時はスループットが最大約30Mbpsとなります。）
- ウイルス検索の対象が使用するポート（25（メール送受信：SMTP）、80（Web：HTTP）、110（メール受信：POP3））についてはIPアドレス／ポートフィルタ機能はご利用できません。

■アップデート設定

セキュリティ対策ファイル（ウイルスパターン、検索エンジン、ファイアウォールルール）をバージョンアップするための各種条件を変更することができます。
取扱説明書の「バージョンアップ」を参照してください。

Webブラウザによる設定について

電話設定

1 画面左メニューの「電話設定」をクリックします。

2 サブメニューが表示されたら、変更したい項目をクリックします。

■サービス設定

サービス設定に関するデータを変更することができます。

1 サブメニューの「サービス設定」をクリックすると現在のデータ内容が表示されます。

2 各項目を設定します。

項　目	内　容	初期値
市外局番	市外局番を入力してください。	なし
加入電話回線種別	加入電話回線の契約（DP/PB）を設定してください。通常は「自動」をご利用ください。 設定範囲：DP/PB/自動	自動
ダイヤル桁間タイマ	最後の番号をダイヤルしてから設定された時間が経過すると、ダイヤル入力の終わりと判定します。 設定範囲：4秒/5秒/6秒/7秒/8秒	4秒
<利用中電話サービス>		
ナンバー・ディスプレイ	ナンバー・ディスプレイ対応電話機と接続する場合は「あり」を選択してください。 設定範囲：なし/あり ※加入電話回線経由でご利用される場合は当社のナンバー・ディスプレイサービスへの契約が必要です。	なし
キャッチホン	当社のキャッチホンに契約している場合はプルダウンメニューから「あり」を選択してください。 設定範囲：なし/あり	なし

（次ページに続く）

Webブラウザによる設定について

項　目	内　容	初期値
<IP電話サービス>		
IP電話サービス	IP電話サービスの無効/有効を設定します。 設定範囲：無効/有効 ※「IP電話設定」を実施すると自動的に「有効」になります。	無効
発信時番号通知	184/186をダイヤルしないでIP電話サービスを利用して電話をかけた場合、お客様の電話番号を相手に通知するか否かを設定します。 設定範囲：非通知/通知	通知
割り込み音	当社のキャッチホンサービスに契約されていないお客様でも、お話中にかかってきた電話があることを音（プップッ…）でお知らせします。フッキングにより通話を切りかえることができます。 ※「キャッチホン」を「あり」と選択した場合は「割り込み音」の選択はできません。 設定範囲：あり/なし	あり

3 着信拒否リストを設定します。

(1) IP電話からの着信について、特定の相手先からの着信を拒否したい場合に設定します。30番号まで登録できます。

(2) 追加方法

①各項目を設定します。

項　目	内　容	初期値
IP電話　着信拒否電話番号	IP電話からの着信拒否を行う相手先電話番号を設定します。 設定範囲：0123456789 # ＊ （48桁以内） 初期値：なし	なし

②「追加」をクリックしてください。次のように一覧に追加されます。
内容が不正な場合は、正しい値を再度入力し「追加」をクリックしてください。

(3) 変更方法

①変更するデータを選択し、データを変更します。

②「変更」をクリックしてください。一覧が更新されます。
内容が不正な場合は、正しい値を再度入力し「変更」をクリックしてください。

(4) 削除方法

削除するデータを選択し「削除」をクリックしてください。
一覧から選択したデータが削除されます。

4 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

5 「送信」をクリックします。

6 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

ワンポイント

● **電話機から追加登録するには**

電話機から「＊＊＊02」とダイヤルすることで追加登録することができます。詳細は「機能仕様」の「着信拒否」(☛P5-3）を参照してください。

● **電話機から登録内容を消去するには**

電話機から「＊＊＊03」とダイヤルすることで登録内容を一斉に消去することができます。詳細は「機能仕様」の「着信拒否」(☛P5-3）を参照してください。

● **Lモードサービスを使用するお客様は**

「ナンバー・ディスプレイ」を「あり」に設定してください。
（当社のLモードサービスへの契約が必要です。）

Webブラウザによる設定について

■ IP電話設定情報

サービスプロバイダ（ISP）に登録されているIP電話に関する基本情報を確認することができます。また、変更することも可能です。

※　本情報の詳細についてはプロバイダ（ISP）にご確認ください。

※　本情報を設定すると自動的にIP電話サービスは「有効」になります。

1 サブメニューの「IP電話設定情報」をクリックすると現在のデータ内容が画面に表示されます。

2 各項目を設定します。

項　目	内　容	初期値
SIPサーバアドレス	IP電話サービスで利用するSIPサーバのIPアドレス、またはFQDN（ホスト名）	なし
SIPサーバポート番号	IP電話サービスで利用するSIPサーバのポート番号	5060
REGISTERサーバアドレス	IP電話サービスで利用するREGISTERサーバのIPアドレス、またはFQDN（ホスト名）	なし
REGISTERサーバポート番号	IP電話サービスで利用するREGISTERサーバのポート番号	5060
SIPドメイン名	ユーザのSIPドメイン名	なし
ユーザID	IP電話サービス用のユーザID	なし
パスワード	IP電話サービス用のユーザパスワード	なし
IP電話番号	ユーザのIP電話番号	なし
市外局番	ユーザの市外局番	なし
アップデート確認用URL	バージョンアップお知らせ用URL 初期値として「http://www.cpeinfo.jp/」が入力されています。プロバイダから特に指定されない場合は変更しないでください。	http://www.cpeinfo.jp/

3 設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

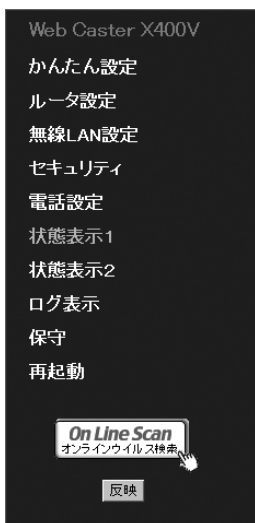
5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

Webブラウザによる設定について

状態表示1

本商品のバージョン情報の確認とプログラムの更新を行うことができます。

1 画面左メニューの「状態表示1」をクリックすると、現在のバージョン情報が表示されます。

2 本商品のバージョン情報を確認します。（30秒毎に最新の状態を表示します。）

各データの説明を次に示します。

（1）装置バージョン

本商品のファームウェアのバージョンアップ情報を表示します。

項　目	内　容
ファームウェアバージョン	本商品のファームウェアバージョン番号を表示します。
アップデート状態	本商品のファームウェアのバージョンアップ情報を表示します。 ①「新しい更新はありません」 本商品に最新版のファームウェアが登録されている状態です。通常はこの表示になります。 ②「更新を確認しています」 サーバへファームウェアの登録情報を確認している状態です。 ③「新しい更新があります。ダウンロードを実行すると、ファームウェアが更新されます」 サーバに最新のファームウェアが登録された状態です。実行時間になると自動的にファームウェア更新を行います。また、「ダウンロード実行」をクリックして、即時更新することも可能です。 ④「新しい更新があります」 ファームウェアの更新が完了していません。「更新確認」をクリックして、最新版のファームウェアを再度確認してください。 ⑤「更新の確認に失敗しました」 サーバのファームウェア登録状況確認が正常終了しなかった状態です。 ⑥「ファームウェアをダウンロード中です」 サーバのファームウェアを本商品にダウンロードしている状態です。 ⑦「ファームウェアのダウンロードに失敗しました」 サーバから本商品へのファームウェアダウンロードが正常に終了しなかった状態です。 ⑧「ファームウェアの更新に失敗しました」 ファームウェア更新が正常終了しなかった状態です。

（次ページに続く）

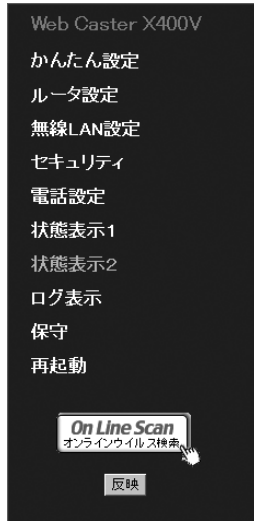
(2) セキュリティバージョン
本商品のセキュリティ対策ファイルのバージョンアップ情報を表示します。

項　目	内　容
検索エンジン	「検索エンジン」の現在のバージョンおよび最新のバージョンを表示します。
ファイアウォールルール	「ファイアウォールルール」の現在のバージョンおよび最新のバージョンを表示します。
ウイルスパターン	「ウイルスパターン」の現在のバージョンおよび最新のバージョンを表示します。
アップデート状態	本商品のセキュリティ対策ファイルのバージョンアップ情報を表示します。 ①「新しい更新はありません」 本商品に最新版のセキュリティ対策ファイルが登録されている状態です。通常はこの表示になります。 ②「更新を確認しています」 サーバへセキュリティ対策ファイルの登録情報を確認している状態です。 ③「新しい更新があります。ダウンロードを実行すると、プログラムが更新されます」 サーバに最新のセキュリティ対策ファイルが登録された状態です。本商品のセキュリティ対策ファイルを更新してください。 ④「更新の確認に失敗しました」 サーバのセキュリティ対策ファイル登録状況確認が正常終了しなかった状態です。 ⑤「プログラムの更新中です」 サーバのセキュリティ対策ファイルを本商品にダウンロードしている状態です。 ⑥「プログラムの更新に成功しました」 セキュリティ対策ファイルの更新が正常終了した状態です。 ⑦「プログラムの更新に失敗しました」 セキュリティ対策ファイル更新が正常終了しなかった状態です。
シリアル番号	フレッツ・セーフティのシリアル番号を表示します。

(3) プログラム手動アップデート
プログラム手動アップデートについては、取扱説明書「バージョンアップ」を参照してください。

状態表示2

本商品の状態を表示することができます。

1 画面左メニューの「状態表示2」をクリックすると、現在の本商品の状態が表示されます。

2 本商品の状態を確認します。（30秒毎に最新の状態を表示します。）

各データの説明を次に示します。

状態表示2　ヘルプ?

動作状態　2005年06月27日 14時10分

DSP状態	正常	WANポート状態	正常
SLIC状態	正常	LAN 1 ポート状態	正常
IP電話回線状態	利用可	LAN 2 ポート状態	異常
加入電話回線状態	利用可	LAN 3 ポート状態	異常
CALLTBL状態	正常	LAN 4 ポート状態	異常

運用設定値

WAN側 MACアドレス	00:80:87:e0:7f:06
LAN側 MACアドレス	00:80:87:e0:7f:86
WAN側取得IPアドレス /マスク長	10.0.0.1/24
WAN側取得デフォルトゲートウェイ	10.0.0.254
SIPサーバIPアドレス	10.10.10.1
加入電話回線種別	DP

PPPoE状態

	接続／切断	状態	取得IPアドレス/マスク長	プライマリDNS セカンダリDNS
接続先1	接続　切断	異常	0.0.0.0/0	0.0.0.0 0.0.0.0
接続先2	接続　切断	未使用	0.0.0.0/0	0.0.0.0 0.0.0.0
接続先3	接続　切断	未使用	0.0.0.0/0	0.0.0.0 0.0.0.0
接続先4	接続　切断	未使用	0.0.0.0/0	0.0.0.0 0.0.0.0
接続先5		未使用	0.0.0.0/0	0.0.0.0 0.0.0.0

（次ページに続く）

Webブラウザによる設定について

（1）動作状態

各所の状態を表示します。右上に本商品に設定されている時刻を表示します。

項　目	内　容
DSP状態	信号変換制御部の状態を表示します。 「正常」：通常は「正常」と表示します。 「異常」：本商品の電源を入れ直してください。それでも「正常」とならない場合は、当社、お問い合わせ先窓口にお問い合わせください。
SLIC状態	TEL制御部の状態を表示します。 「正常」：通常は「正常」と表示します。 「異常」：本商品の電源を入れ直してください。それでも「正常」とならない場合は、当社、お問い合わせ先窓口にお問い合わせください。
IP電話回線状態	IP電話サービスの利用状況を表示します。 「利用可」　：利用可能（通話待ち）です。 「利用中」　：通話中です。 「利用不可」：利用不可能です。「4　お困りのときには」（☛P4-2） 「利用停止」：利用停止しています。「機能仕様」の「IP電話サービス利用停止」（☛P5-4）
加入電話回線状態	加入電話回線の利用状況を表示します。 「利用可」　：利用可能（通話待ち）です。 「利用中」　：通話中です。 「直結中」　：加入電話回線のみご利用可能な状態です。（IP電話サービスはご利用できません。）「通話／ダイヤルに関するトラブル」（☛P4-3） 「利用不可」：利用できません。電話機コードが抜けている可能性があるので、取扱説明書「回線を接続する」を参照して本商品と加入電話回線が正常に接続されていることを確認してください。また本商品の起動直後はこの状態となります。この場合はしばらくお待ちください。
CALLTBL状態	IP電話回線と加入電話回線の回線選択データベースの状態を表示します。 「正常」：通常は「正常」と表示します。 「異常」：本商品の電源を入れ直してください。それでも「正常」とならない場合は、当社、お問い合わせ先窓口にお問い合わせください。
WANポート状態	WAN側インタフェースのリンク状態を表示します。 「正常」：回線が正常に接続されています。 「異常」：回線の接続が異常または未使用の状態です。
LAN1ポート状態	LAN1側インタフェースの各リンク状態を表示します。 「正常」：回線が正常に接続されています。 「異常」：回線の接続が異常または未使用の状態です。
LAN2ポート状態	LAN2側インタフェースの各リンク状態を表示します。 「正常」：回線が正常に接続されています。 「異常」：回線の接続が異常または未使用の状態です。
LAN3ポート状態	LAN3側インタフェースの各リンク状態を表示します。 「正常」：回線が正常に接続されています。 「異常」：回線の接続が異常または未使用の状態です。
LAN4ポート状態	LAN4側インタフェースの各リンク状態を表示します。 「正常」：回線が正常に接続されています。 「異常」：回線の接続が異常または未使用の状態です。

（2）運用設定値

装置情報を表示します。

項　目	内　容
WAN側MACアドレス	本商品のWAN側のMACアドレスを表示します。
LAN側MACアドレス	本商品のLAN側のMACアドレスを表示します。
WAN側取得IPアドレス/マスク長	本商品のWAN側が取得しているIPアドレスおよびサブネットマスクを表示します。
WAN側取得デフォルトゲートウェイ	本商品のWAN側が取得しているデフォルトゲートウェイを表示します。
SIPサーバIPアドレス	本商品が使用しているSIPサーバのIPアドレスを表示します。
加入電話回線種別	接続している電話回線の回線種別を表示します。 ダイヤルパルス回線の場合：「DP」 プッシュホン回線の場合　：「PB」 回線種別が未決定の場合　：「不明」

（3）PPPoE状態

●状態表示

PPPoE接続状態を表示します。

項　目	内　容
状態（接続先1〜5）	各接続先の状態を表示します。 「正常」　　：インターネットに接続できます。 「異常」　　：インターネットに接続できていません。「パソコンに関するトラブル」（☛P4-4） 「認証エラー」：PPPの認証エラーです。インターネットに接続できていません。「設定に関するトラブル」（☛P4-2） 「未使用」　：PPPoEを利用していない状態です。
取得IPアドレス/マスク長（接続先1〜5）	それぞれの接続先のPPPoE設定で取得しているIPアドレス、マスク長およびデフォルトゲートウェイのアドレスを表示します。
プライマリDNS セカンダリDNS （接続先1〜5）	それぞれの接続先のPPPoE設定で取得しているプライマリDNSおよびセカンダリDNSのIPアドレスを表示します。

（次ページに続く）

Webブラウザによる設定について

●手動接続

PPPoEへの接続/切断を指示します。PPPoE設定「セッション設定」で「使用するセッション」の「接続」/「切断」を指示することができます。

PPPoE状態

	接続／切断
接続先1	接続 切断
接続先2	接続 切断
接続先3	接続 切断
接続先4	接続 切断
接続先5	

①本機能を実施する前に、接続先のPPPoE状態をメニューの「状態表示2」でご確認ください。

・「正常」の場合→「切断」をクリックするとPPPoEを切断します。

・「正常」以外の場合→「接続」をクリックするとPPPoEを接続します。

②ボタンをクリックすると結果を表示します。

例：「接続先1」の「接続」をクリックし接続が正常終了した場合（無通信監視タイマ：無効）：

状態表示2　ヘルプ?

PPPoE手動接続

実行セッション	接続先1
実行内容	接続

結果

接続完了

PPPoEの接続が正常に行われました。

戻る

<table>
<tr><th>項　目</th><th>内　容</th></tr>
<tr><td rowspan="2">PPPoE 手動接続</td><td>接続：接続完了：
PPPoEの接続が正常に行われました。
設定完了：
PPPoEの無通信監視の設定が完了しました。
接続するPPPoEの「無通信監視タイマ」に時間を指定したときは「接続」をクリックしただけではPPPoEへの接続は行いません。
「無通信監視タイマ」によるセッションの切断監視が可能になります。
接続失敗：
ネットワークに問題があるため、PPPoEの接続が行えませんでした。しばらく待ってもう一度お試しください。この問題が続くときは、当社、お問い合わせ先窓口にお問い合せください。同じ操作を実施すると「すでに接続中」と表示される場合がありますが、接続は正常におこなわれていますので、問題はありません。そのまま、ご利用ください。
認証エラー：
「PPPoE設定」画面「インターネットサービスプロバイダ設定」で設定した接続先情報が正しく設定されていません。設定内容をご確認の上、もう一度お試しください。
接続処理中：
現在、接続中です。しばらく待って「状態表示2」画面の「PPPoE状態」をご確認ください。
既に接続中：
既にPPPoEが接続されています。「状態表示2」画面の「PPPoE状態」をご確認ください。
エラー：
「PPPoE設定」画面「セッション設定」および「インターネットサービスプロバイダ設定」で設定した接続情報または接続先情報が設定されていません。設定後、もう一度お試しください。</td></tr>
<tr><td>切断：切断完了：
PPPoEの切断が正常に行われました。
未接続：
PPPoEの接続が行われていません。
※「動作モード」が「PPPoE」以外の場合に実施すると本表示となります。
通話中：
通話中のため、PPPoEの切断を行うことができません。通話を終了してから、もう一度実行してください。
切断処理中：
現在、切断中です。しばらく待って「状態表示2」画面の「PPPoE状態」をご確認ください。</td></tr>
</table>

お知らせ

- PPPoE設定で「接続先1～4」の情報を変更し、「確認」「送信」のあとに接続確認を行い、接続できることが確認できても「反映」でシステム更新しないと本商品に反映されないのでご注意ください。
- 「接続完了」後、ファームウェアの自動バージョンアップが行われる場合があります。

（次ページに続く）

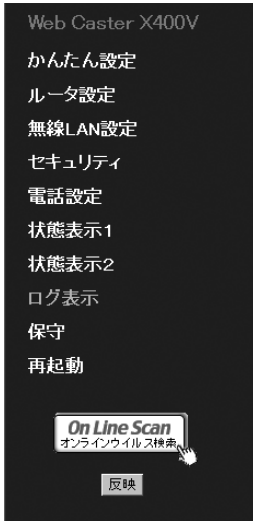
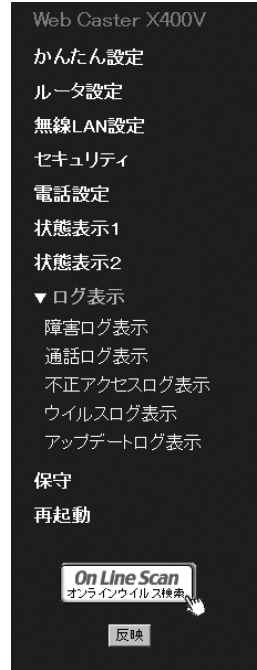
Webブラウザによる設定について

ランプの種類	ランプのつき方
POWER	点灯（緑）
ALARMランプ	消灯
PPPランプ	消灯：オフライン状態（セッション未接続） 点灯（緑）：1セッション接続時 点灯（橙）：2セッション以上接続時
VoIPランプ	点灯（緑）
TELランプ	点灯（橙）
WANランプ	点灯（緑）または点滅（緑）
HACKERランプ	点灯（緑）
VIRUSランプ	点灯（緑）

③「戻る」をクリックしてください。（「状態表示2」画面に戻ります。）
※「接続先1～4」の接続先情報を変更したい場合は「切断」をクリック後、「PPPoE設定」画面「インターネットサービスプロバイダ設定」のアカウントを変更して、「接続」をクリックしてください。

ログ表示

本商品の利用状況を表示することができます。

1 画面左メニューの「ログ表示」をクリックします。

2 サブメニューが表示されたら、変更したい項目をクリックします。

Webブラウザによる設定について

■障害ログ表示

本商品の障害状況を表示することができます。

（注）本商品に異常があった場合に実施する操作です。当社から指示がない限り操作する必要はありません。
ログ内容に関するお問い合わせにはお答えできません。

1 サブメニューの「障害ログ表示」をクリックします。

【注1】分類コード
- 00（Fault）　：障害
- 01（Report）　：通知
- 10（Remove）：復旧

【注2】装置コード　障害の発生箇所。
【注3】詳細コード　装置コード毎の種別。
【注4】SEQ番号　障害の発生した位置（セッション番号など）を示します。
【注5】ログが出力された日時

［フォーマット］

【注1】	【注2】	【注3】	【注4】	【注5】
AA(aaa)	BB(bbb)	CC(cccc)	SEQ=dd	www mmm dd hh:mm:ss yyyy
	XXXXXXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX　XXXXXXXX

■通話ログ表示

本商品の通話状況を表示することができます。

1 サブメニューの「通話ログ表示」をクリックします。

【注1】発着信日時
【注2】通話開始日時
【注3】通話終了日時
【注4】本商品の電話番号（IP電話番号（050）を表示します。）
【注5】電話サービス使用状況　VoIP:IP電話/PSTN:加入電話
【注6】発着信 ORG=発信（電話をかけた）/TRM=着信（電話がかかってきた）
【注7】相手先電話番号

［フォーマット］

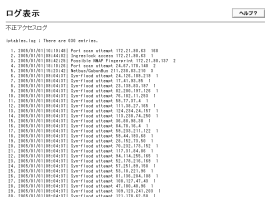
【注1】　www mmm dd hh:mm:ss yyyy
【注2】　www mmm dd hh:mm:ss yyyy
【注3】　www mmm dd hh:mm:ss yyyy
【注4】　AAAAAAAAAA
【注5】　BBBB
【注6】　CCC XX XXX XXX
【注7】　DDDDDDDDDD

XXX.XXX.XXX.XXX XXXXX

XXX/　XXX/　XXX　XXX/　XXX　XXX
XXX　XXX　XXX　XXX　XXX　XXX

■不正アクセスログ表示

本商品の不正アクセス状況を表示することができます。
不正アクセスログでは、コンピュータやネットワークに対する、不正アクセスの疑いのあるアクセスの記録を保持し、最近の不正アクセスからさかのぼって最大30件の不正アクセスが記録されます。

1 サブメニューの「不正アクセスログ表示」をクリックします。

【注1】ログが出力された日時
【注2】不正アクセス種別
【注3】アクセス元のIPアドレス
【注4】アクセス回数（不正アクセス種別およびアクセス元のIPアドレスが一致した場合は本フィールドのみ更新されます。）

※HACKERランプが赤点灯しているときは、本メニューを表示すると元の表示に戻ります。

［フォーマット］

【注1】	【注2】	【注3】	【注4】
yyyy/mm/dd│hh:mm:ss│	AAAAAAAAAAAAAA	BBB.BBB.BBB.BBB	CC

■ウイルスログ表示

本商品のウイルス検出状況を表示することができます。
ウイルスログでは、送受信されるe-mailメッセージから検出されたウイルスの記録を保持し、最近検出されたウイルスからさかのぼって最大30件までのウイルス検出が記録されます。
「ウイルスログ表示」画面には、最近検出されたウイルスについて、検出日時、e-mail送信者、e-mail受信者、ウイルス検出時の処理、ウイルスに感染していたファイル名、検出されたウイルス名が表示されます。

1 サブメニューの「ウイルスログ表示」をクリックします。

※VIRUSランプが赤点灯しているときは、本メニューを表示すると元の表示に戻ります。

【注1】ログが出力された日時
【注2】FROMヘッダの内容 または "Webmail"
【注3】TOヘッダの内容 または "Webmail"
【注4】添付ファイル名
【注5】検出時に実施した対策結果
"ウイルス駆除"：感染ファイルからウイルスコードを除去しました。
"削除"：感染ファイルまたは不正コード（トロイの木馬、ワームなど）を含むファイルを削除しました。
"放置"：本ログファイルへ感染ファイルの記録を行いました。感染ファイルには対策は行わず放置してあります。
"ウイルス駆除不能(削除)"： 感染ファイルの駆除に失敗したので、感染ファイルは削除しました。
"ウイルス駆除不能(放置)"： 感染ファイルの駆除に失敗したので、感染ファイルは放置してあります。
"検出"： ウイルスを検出しました。通知された指示に従って処置してください。
【注6】検出したウイルス名

［フォーマット］

【注1】	【注2】	【注3】	【注4】	【注5】	【注6】
yyyy/mm/dd│hh:mm:ss│ ID=XXXXX	&from=YYYYY	&to=ZZZZZ	&file=AAAAAAA	&action=BBBBBBBBBB	&virus=CCCCCCC

Webブラウザによる設定について

■アップデートログ表示

本商品のバージョンアップ状況を表示することができます。
アップデートログでは、本商品のプログラムの更新状況の記録を保持し、最新のバージョンアップからさかのぼって最大30件までが記録されます。
「アップデートログ」画面には、最近実行されたバージョンアップの日付、ファームウェアおよび各セキュリティ対策ファイルのバージョン番号などが表示されます。

1 サブメニューの「アップデートログ表示」をクリックします。

ログ表示　ヘルプ？

アップデートログ

```
updatelog.log : There are 005 entries.

  1. 2005/01/01|09:01:05| **.**.**** *.*** *.***.** *** INITIAL
  2. 2005/01/01|09:01:41| **.**.**** *.*** *.***.** *** MANUAL
  3. 2005/01/01|12:30:52| **.**.**** *.*** *.***.** *** AUTO
  4. 2005/01/01|13:00:24| **.**.**** *.*** *.***.** *** LOCAL
  5. 2005/01/02|09:01:05| **.**.**** *.*** *.***.** *** TEL
```

【注1】ログが出力された日時
【注2】バージョンアップ後のファームウェアのバージョン
【注3】バージョンアップ後のウイルス検索エンジンのバージョン
【注4】バージョンアップ後のパターンファイル番号
【注5】バージョンアップ後のファイアウォールルール番号
【注6】バージョンアップ種別

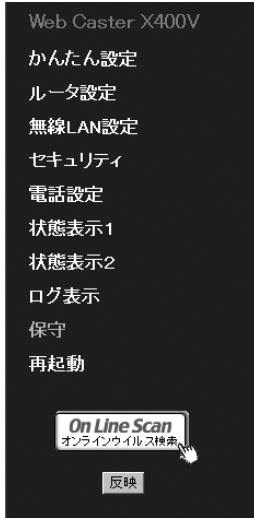
［フォーマット］

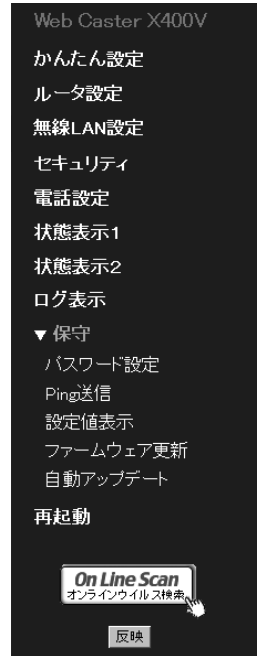
【注1】	【注2】	【注3】	【注4】	【注5】	【注6】
yyyy/mm/dd|hh:mm:ss|	XXX.YYY.ZZZ	AA.BB	CC	DD	EE

お知らせ

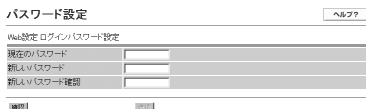
●フォーマットは予告なく変更される場合があります。
●お客様のご利用状況によっては、各ログ表示内容が消去される場合があります。

保守

1 画面左メニューの「保守」をクリックします。

2 サブメニューが表示されたら、保守を実施したい保守項目をクリックします。

Webブラウザによる設定について

■パスワード設定

Web設定ログインパスワードを変更することができます。

1 サブメニューの「パスワード設定」をクリックします。

2 各項目を設定します。

項　目	内　容	初期値
<Web設定ログインパスワード設定>		
現在のパスワード	現在使用しているパスワードを入力します。	なし
新しいパスワード	新しいパスワードを設定します。 設定範囲：1〜10文字以内、半角英数字およびASCIIコードの記号（ただし、「"」「；」スペースを除く） ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。.	なし
新しいパスワード確認	確認のため、もう一度「新しいパスワード」を設定してください。	なし

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 「送信」をクリックします。

ネットワークパスワード入力画面が表示されます。

5 ユーザー名（admin）および新しいパスワードを入力してください。

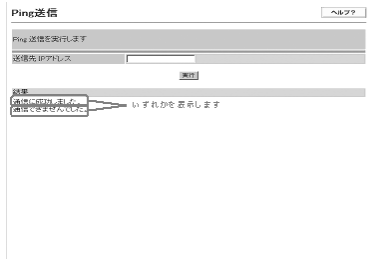
お知らせ

●「反映」をクリックせずにシステム更新、または電源を切った場合、新しいパスワードが本商品に反映されませんのでご注意ください。

■Ping送信

相手装置にPingを送信して正常に接続されていることを確認することができます。

（注）本商品に異常があった場合に実施する操作です。当社から指示がない限り操作する必要はありません。

サブメニューの「Ping送信」をクリックします。

2 各項目を設定します。

項　目	内　容
送信先IPアドレス	Pingの送信先IPアドレスを設定します。 設定後、「実行」をクリックしてください。（Ping送信されます。）結果が表示されます。 相手先と正常に通信が行われている場合→「通信に成功しました。」 相手先と正常に通信が行われていない場合→「通信できませんでした。」

■設定値表示

設定データの内容を1つの画面で確認できます。

（注）本商品に異常があった場合に実施する操作です。当社から指示がない限り操作する必要はありません。

1 サブメニューの「設定値表示」をクリックします。

初期値と異なるデータを表示します。

```
SECURITY         1 myid ***** ;
VOIP_TELNUM      0884118 ;
NET_DOMAIN       mydomain.ntt.co.jp ;
REGIST_DOMAIN    sip.ntt.co.jp ;
PROXY_DOMAIN     sip.ntt.co.jp ;
```

■ファームウェア更新

取扱説明書「バージョンアップ」を参照してください。

■自動アップデート

ファームウェアの自動バージョンアップに関する設定を確認できます。「ファームウェア更新確認情報設定」画面の「自動アップデート機能設定」と同じ内容になります。（取扱説明書「バージョンアップ」）

Webブラウザによる設定について

再起動

本商品の再起動の仕方は取扱説明書「再起動」を参照してください。

Webブラウザによる設定の終了

1 Webブラウザの[ファイル]-[閉じる]をクリックまたは、画面右上の ☒ をクリックします。

設定を変更した場合、Webブラウザを終了する前に「反映」をクリックし、設定内容を本商品に反映させてください。

セキュリティ設定

「セキュリティ」機能の有効/無効を選択することができます。
本設定を行うにはWebブラウザのアドレス(D)欄に「http://setup.fletsphone/security.html」を入力して、設定画面を呼び出す必要があります。

1 「セキュリティ設定」画面を表示します。

Webブラウザのアドレス(D)欄に「http://setup.fletsphone/security.html」を入力し、「ENTER」キーを押してください。

2 本商品へログインします。

ネットワークパスワード入力画面からユーザー名（admin)、初期設定で登録したパスワードを入力してください。

3 現在の「セキュリティ設定」のセキュリティ無効/有効の選択状態を表示します。

4 現在のセキュリティ設定に変更を入れる場合はラジオボタンを設定します。

項　目	内　容	初期値
<セキュリティ設定>		
セキュリティ無効/有効	「無効」選択時：検索エンジン/ファイアウォールルール/ウイルスパターンの3ファイルは更新しません。ウイルス検索と攻撃検知機能も動作しません。 「有効」選択時：検索エンジン/ファイアウォールルール/ウイルスパターンの3ファイルは更新されます。ウイルス検索と攻撃検知機能も動作します。	有効

5 「確認」、「送信」をクリックします。

（次ページに続く）

Webブラウザによる設定について

6 「かんたん設定」画面を表示します。

Webブラウザのアドレス(D)欄に「http://192.168.1.1」を入力し、「ENTER」キーを押してください。

7 「反映」をクリックしてください。システム更新を行い、「HACKERランプ/VIRUSランプ」が以下の点灯状態になっていることを確認してください。

「セキュリティ設定」無効選択時：

ランプの種類	ランプのつき方
ALARMランプ	消灯
PPPランプ	点灯（橙）または点灯（緑）
WANランプ	点灯（緑）または点滅（緑）
HACKERランプ	消灯
VIRUSランプ	消灯

「セキュリティ設定」有効選択時：

ランプの種類	ランプのつき方
ALARMランプ	消灯
PPPランプ	点灯（橙）または点灯（緑）
WANランプ	点灯（緑）または点滅（緑）
HACKERランプ	点灯（緑）※1
VIRUSランプ	点灯（緑）※2

※1　HACKERランプは「不正アクセスレベル」が「低」の設定の場合は「セキュリティ設定」有効選択時でも「消灯」となります。

※2　VIRUSランプは「Eメールウイルス検索」および「Webメールウイルス検索」の両方が「無効」の場合「セキュリティ設定」有効選択時でも「消灯」となります。

お知らせ

●セキュリティ無効／有効を「無効」にすると、フレッツ・セーフティの機能がご利用できなくなります。

3 無線LANを利用する

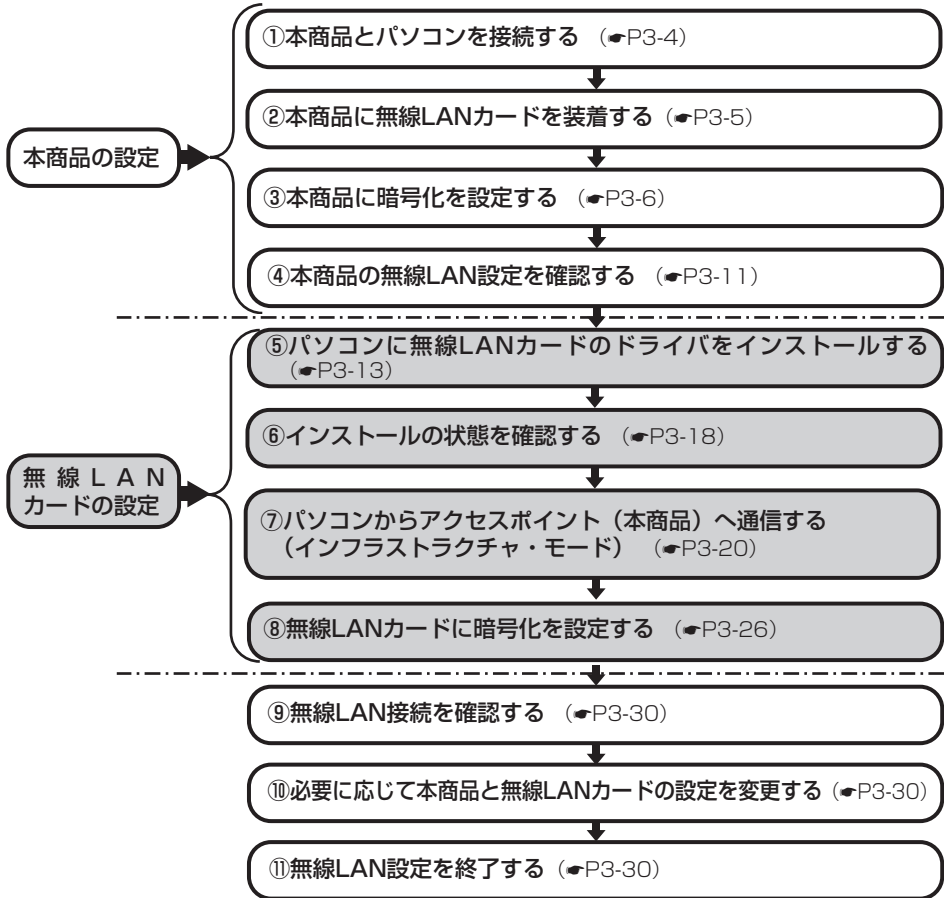
本商品を無線LANのアクセスポイントとして
利用する場合の設定について説明します。

LANケーブルを使用した設定・・・・・・・・・3-2
本商品とパソコンの設定 ・・・・・・・・・・・・・3-4
LANケーブルを使用しない設定 ・・・・3-31

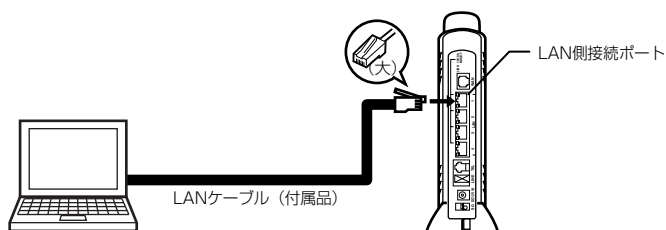
LANケーブルを使用した設定

本商品を無線LANアクセスポイントとして利用する場合の設定について説明します。
本商品の無線LAN機能を使用するには、専用の無線LANカード（Web Caster FT-STC-Va/gまたはWeb Caster FT-STC-Oa/g 無線LANカード（以下、「無線LANカード」といいます））が必要となります。
本章は無線LANカードがWeb Caster FT-STC-Va/gのご使用を前提で記載します。

※1 Web Caster FT-STC-Oa/gをご使用の場合、「無線LANカードの設定」については「Web Caster FT-STC-Oa/g 取扱説明書」または「Web Caster FT-STC-Oa/g 詳細取扱説明書」を参照してください。
※2 パソコンのOSに「Windows® 2000/XP」をご使用の場合は、「Web Caster X400V まるごと設定ツールの使い方」を参照してください。
※3 まるごと設定ツールを使用してドライバ・ユーティリティがインストールできない場合、またはパソコンのOSに「Windows® 2000/XP以外」をご使用の場合は、本章をご覧ください。
パソコンのOSにWindows® XPをご使用の場合
→本章を参照してください。
パソコンのOSにWindows® XP以外をご使用の場合
→本章の「無線LANカードの設定」については、無線LANカードの「詳細取扱説明書」を参照してください。
※4 無線LANカードのドライバ・ユーティリティは変更される場合があります。
そのときはホームページからドライバ・ユーティリティおよび設定マニュアルを入手してください。
※次ページに示した手順の流れは、パソコンと本商品をLANケーブルで接続して本商品と無線LANカードを設定する基本的な方法になります。LANケーブルを使用しないで設定する場合は本章末尾の「LANケーブルを使用しない設定」（☛P3-31）を参照してください。

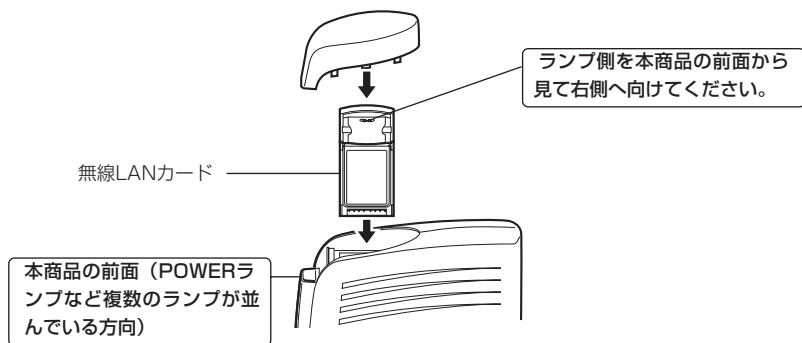
本商品の設定
①本商品とパソコンを接続する （☛P3-4）
②本商品に無線LANカードを装着する（☛P3-5）
③本商品に暗号化を設定する （☛P3-6）
④本商品の無線LAN設定を確認する （☛P3-11）
無線LAN
カードの設定
⑤パソコンに無線LANカードのドライバをインストールする
（☛P3-13）
⑥インストールの状態を確認する （☛P3-18）
⑦パソコンからアクセスポイント（本商品）へ通信する
（インフラストラクチャ・モード） （☛P3-20）
⑧無線LANカードに暗号化を設定する （☛P3-26）
⑨無線LAN接続を確認する （☛P3-30）
⑩必要に応じて本商品と無線LANカードの設定を変更する（☛P3-30）
⑪無線LAN設定を終了する（☛P3-30）

本商品とパソコンの設定

①本商品とパソコンを接続する

パソコンのLANポートと本商品背面のLAN側接続ポートを本商品付属のLANケーブルで接続してください。

●本商品に接続するパソコンはCD-ROMドライブを内蔵しているものをご使用ください。（お使いのパソコンがCD-ROMドライブを内蔵していない場合は、CD-ROMドライブもご用意ください。）
また、本商品に接続するパソコンが以下の条件を満たすものであることをご確認ください。

PCカードスロット	インタフェース	PC Card Standard（CardBus）・Type Ⅱ
	使用電源	DC3.3V±5%（パソコンから供給） DC5V 仕様のPC カードスロットではお使いになれません。
OS		Windows® 98SE／Windows® Me／Windows® 2000 Professional／Windows® XP（日本語版） ※Mac OS はご利用になれません。

②本商品に無線LANカードを装着する

まず、本商品の電源を切ってください。
本商品の無線LAN カードスロットに無線LAN カードを装着し、本商品の電源を入れてください。

お知らせ

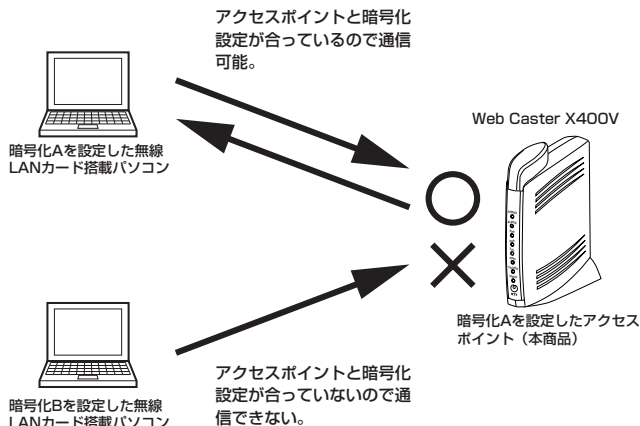
●無線LANカードは正しい向きで挿入してください。誤った方向で挿入すると本商品や無線LANカードが破損する可能性があります。
●無線LANカードの装着後、本商品に電源を入れてから6分～10分の間はインターネットがご利用になれません。
●本商品の電源を切る前に、Webブラウザで本商品にログインし、「状態表示2」画面の「PPPoE手動接続」で「切断」をクリックすれば、次回電源を入れたときにすぐインターネットをご使用いただけます。「PPPoE設定」（☛P2-11）
●本商品から無線LANカードを外すときには、必ず本商品の電源を切ってから外してください。

本商品とパソコンの設定

③本商品に暗号化を設定する

アクセスポイント（本商品）に暗号化の設定を行います。
無線LAN通信は、電波を使用しているため、ケーブルの配線が不要というメリットがあります。ただし、通信内容の暗号化をしていない場合には、電波の届く範囲であれば通信内容を傍受される危険性が考えられます。
そのため、無線LANをご利用になる場合は必ず暗号化（WEP/WPA）の設定を行ってください。なお、無線LANカードでサポートしているWPAの暗号化プロトコルはTKIPのみとなります。

●WEP(Wired Equivalent Privacy)
無線LAN規格（IEEE802.11）で規格化されている暗号化方式の一つです。直訳は、“有線LANと同等のプライバシー機能”となり、無線LANに対するセキュリティの有効な手段とされています。WEPを設定することで、無線電波が第三者に傍受されても、暗号を解読しないとデータの中身を判読することができなくなり、また無線LANに侵入することもできません。WEP機能は、パソコン等および無線LANアクセスポイント側の両方に『WEPキー（WEP暗号化鍵）』を設定する必要があります。本商品は、64ビットおよび128ビット長のWEPキーをサポートしています。各ビット長のうち、お客様が設定できるWEPキー長は、それぞれ「40 bit (5 byte)」、「104 bit (13 byte)」となります。残りの24ビットはIV（Initialization Vector）といわれる自動的にパソコンや無線LANアクセスポイントにより付加されるデータとなります。設定されるWEPキーの長さが長いほど、暗号は強力なものとなります。

●WPA（Wi-Fi Protected Access）
WPAとは、WEPの脆弱性を改善した暗号化方式です。
ユーザ認証機能の追加や、「PSK（事前共有キー）」を元に作成する暗号キーを一定時間ごとに自動的に更新するTKIP（Temporal Key Integrity Protocol）と呼ばれる暗号化プロトコルを採用することにより、セキュリティ強度が向上します。

アクセスポイント（本商品）の暗号化設定

1 **Webブラウザで本商品にログインし、メニューの「無線LAN設定」をクリックし、サブメニューの「暗号化設定」をクリックしてください。**

下記画面が表示されます。暗号化設定を行ってください。
以下では、暗号方式に「TKIP+PSK」を選択し、「PSK（事前共有キー）」に「abcdefgh」、「キーリフレッシュタイマ」（暗号キーの更新周期）を「10分」に設定した場合の例を示します。
設定した「PSK（事前共有キー）」はお手元に記録しておいてください。

（次ページに続く）

本商品とパソコンの設定

2 暗号化方式を選択し、必要な項目を設定します。

項 目	内 容	初期値
暗号方式 ※ここでは、「TKIP+PSK」を選択します。	データの暗号方式の種別を設定します。 「OFF」：暗号化を行いません。 「WEP」：「WEP」項目の設定を行ってください。 「TKIP+PSK」：「WPA-PSK情報」項目の設定を行ってください。 セキュリティ強度はOFF < WEP < TKIP+PSKの順に高くなります。 設定範囲：OFF/WEP/TKIP+PSK	OFF
<WEP>		
WEPキータイプ	WEPキータイプの方式を設定します。 「自動設定（Pass Phrase)」を選択： 「WEPキー Pass Phrase」項目にPass Phraseデータを設定してください。 「直接入力」を選択： 「WEPキー設定情報」項目にWEPキーデータを設定してください。 設定範囲：自動設定（Pass Phrase）/直接入力	自動設定 （Pass Phrase）
暗号化ビット長	WEPキーのビット長を設定します。WEPキーのビット長が長いほど、セキュリティレベルは高くなります。 設定範囲：64/128	64
WEPキー Pass Phrase	WEPキー のPass Phrase（パスワードを長くしたもの）を設定します。設定後に「WEPキー 生成」をクリックしてください。WEPキーを生成します。 暗号化ビット長 ：64選択時：4種類のキーを生成 （「WEPキー1」～「WEPキー4」にキー情報が入ります。） ：128選択時：1種類のキーを生成 （「WEPキー1」～「WEPキー4」には同じキー情報が入ります。） 使用可能文字：1～31文字、半角英数字およびASCIIコードの記号（ただし、「"」「；」スペースを除く） ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。	なし

項　目	内　容	初期値
<WEPキー設定情報>		
入力方式	WEPキーの形式を選択します。 使用可能文字：文字入力／16進数（HEX）入力 ※文字入力とは半角英数字およびASCIIコードの記号（ただし、「”」「；」を除く）で入力し、16進数（HEX）入力とは例えば123abc のような0～9 の数字とA～F（またはa～f）のアルファベットで表現された数値で入力する方法です。 ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。	16進数（HEX）入力
デフォルト送信キー	下記WEPキー1～4のどれを使用するか選択します。 設定範囲：1～4	1
WEPキー1 WEPキー2 WEPキー3 WEPキー4	キータイプが文字入力の場合： 使用可能文字：半角英数字およびASCIIコードの記号 （ただし、「"」「;」スペースを除く） 暗号化ビット長：64選択時　：5桁 128選択時　：13桁 キータイプが16進数（HEX）入力の場合： 使用可能文字：A～F、0～9、a～f 暗号化ビット長：64選択時　：10桁 128選択時　：26桁 ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。	なし
<WPA-PSK情報>		
PSK（事前共有キー） ※ここでは「abcdefgh」と入力します。（お客様が設定する際は、任意の値を入力してください。）	PSK（事前共有キー）を設定します。 PSK（事前共有キー）として任意の文字列を設定します。このキーを元に「キーリフレッシュタイマ」の設定時間ごとに暗号を自動的に変更します。 使用可能文字：8～63文字、半角英数字およびASCIIコードの記号 （ただし、「"」「；」スペースを除く） ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。	なし
キーリフレッシュタイマ ※ここでは、「10」と入力します。	暗号鍵の更新時間を設定します。 設定範囲：0（リフレッシュなし）、1～60（分）	0

3 すべての設定が終了したら「確認」をクリックします。

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

（次ページに続く）

本商品とパソコンの設定

4 「送信」をクリックします。

5 「反映」をクリックします。

システム更新終了後、設定した内容が有効になります。

お知らせ

●設定を変更する場合は無線LANカードを装着したパソコンの設定も変更してください。変更しないと通信できなくなります。

④本商品の無線LAN設定を確認する

アクセスポイント（本商品）の基本設定を確認します。

1 Webブラウザで本商品にログインし、メニューの「無線LAN設定」をクリックし、サブメニューの「基本設定」をクリックしてください。

下記画面が表示されます。ESSIDの欄に表示されている内容をお手元に記録しておいてください。

ESSIDをお手元に記録します

2 必要に応じて「基本設定」を変更します。

項　目	内　容	初期値
無線動作モード	無線動作モード種別を設定します。 設定範囲：11b+g（IEEE802.11bおよびIEEE802.11g） 11g（IEEE802.11g）/ 11a（IEEE802.11a）	11b+g
ESSID ※これをお手元に記録しておいてください。ここでは「X400V-0123ad」となっています。	無線LAN機器が、通信するお互いを識別するIDとしてネットワーク名（ESSID）を設定します。このネットワーク名が一致しないと無線通信ができません。 初期状態は「X400V-xxxxxx」xxxxxxは本商品のMACアドレスの下6桁となっています。 一般にネットワーク名は検索することができますので、セキュリティ上、他のパソコンからのアクセスを防止するため、一定期間ごとに変更することを推奨します。 設定範囲：1～32文字、半角英数字およびASCIIコードの記号（ただし、「"」「；」スペースを除く） ※ASCIIコードの詳細については取扱説明書「ASCIIコード表」を参照してください。	X400V-xxxxxx（xxxxxxは本商品のMACアドレス下6桁）
ANY接続 ※「拒否」に設定することを推奨します。	無線LANクライアントからのANY接続を許可するかどうかを設定します。 設定範囲：拒否/許可	拒否
送信パワー設定	送信パワーを設定します。 設定範囲：100/50/25（%）	100

お知らせ

●IPv6サービス（「IPv6ブリッジ設定」＝「有効」）とIEEE802.11bおよびIEEE802.11g（「無線動作モード」＝「11b+g」）を同時に利用すると、無線LANクライアント側のパソコンでインターネットに接続できなかったり、通信が切れる場合があります。（「ネットワーク設定」（☛P2-8））

（次ページに続く）

本商品とパソコンの設定

項　目	内　容	初期値
<無線チャンネル>		
2.4GHz帯	2.4GHz帯の設定をします。 設定範囲：1～13（チャンネル）	7
5.0GHz帯	5.0GHz帯の設定をします。 設定範囲：34/38/42/46（チャンネル）	34
<速度設定>		
11b+g	通信速度を自動設定します。（auto）	auto
11g	設定範囲： auto/54/48/36/24/18/12/9/6	auto
11a	設定範囲： auto/54/48/36/24/18/12/9/6	auto

3 **すべての設定が終了したら「確認」をクリックします。**

内容が不正な場合は、正しい値を再度入力し「確認」をクリックしてください。正しい値を入力した場合は「送信」が有効になります。

4 **「送信」をクリックします。**

5 **「反映」をクリックします。**

システム更新終了後、設定した内容が有効になります。

お知らせ

- 設定を変更する場合は無線LANカードを装着したパソコンの設定も変更してください。変更しないと通信できなくなります。
- ESSIDとは、本商品と無線LANカードとが通信時に使用するネットワーク識別用のIDです。本商品にESSIDを設定しておき、接続するパソコン等にも同じESSIDを設定しておけば、通信が可能になります。このように、接続する本商品をESSIDで指定することができます。ESSIDは、セキュリティ機能の一つに分類される場合もありますが、あくまでも接続先の識別機能ですので、ESSIDを設定後に、他のセキュリティ設定をすることをお勧めします。
- ANY接続とは、無線LANクライアントの設定で、接続先アクセスポイントのESSIDを空欄または「ANY」に設定した場合に、ESSIDが一致しなくてもアクセスポイントに接続が可能になる方法のことです。ANY接続を「許可」に設定しておくと、アクセスポイントのESSIDがわからなくとも接続が可能ですので、セキュリティ面から見ると好ましくなく、アクセスポイント（本商品）側でANY接続を「拒否」にすることをお勧めします。ANY接続を「拒否」に設定している場合は、本商品に設定されているESSIDを指定しないと接続する事はできません。また、アクセスポイント側にWEPキー等の暗号化設定がなされている場合、設定内容を一致させないと通信を行うことはできません。

⑤パソコンに無線LANカードのドライバをインストールする

ここからは無線LANカードの設定になります。

※以降は無線LANカードに「Web Caster FT-STC-Va/g」を使用した場合で説明しています。「Web Caster FT-STC-Oa/g」を使用する場合は無線LANカードのCD-ROMに収録されている「詳細取扱説明書」を参照してください。

パソコンに無線LANカードのドライバをインストールします。

※以降はOSにWindows® XPを使用した場合で説明しています。
他のOSをご使用になるときは専用の無線LANカードのCD-ROMに収録されている詳細取扱説明書を参照してください。(「Web Caster FT-STC-Va/g詳細取扱説明書」の「ドライバをインストールしましょう」)

●インストールする際には以下の点にご注意ください。

・CD-ROMをドライブにセットしてもメニュー画面が表示されない場合

「スタート」ー「マイコンピュータ」をクリックして、「FT-STC-Va_g」アイコンをダブルクリックしてください。CD-ROMの内容が表示されますので「FT-STC-Va_g.exe」をダブルクリックするとメニュー画面が表示されます。

・インストールを行う前に、全てのアプリケーションを終了させてください。

・無線LANカードはスタンバイモードには対応していません。
インストールする前に、ご使用のパソコンの取扱説明書等をお読みになり、スタンバイモードを解除しておいてください。

お知らせ

● ウイルスチェックプログラムが起動している状態でインストールを行うと正常にインストールが完了しない場合があります。インストール作業はウイルスチェックプログラムを一時的に終了してから行ってください。

本商品とパソコンの設定

1 パソコンの電源を投入し、Windows® XPを起動します。その際、必ずAdministrator権限のあるユーザでログインしてください。

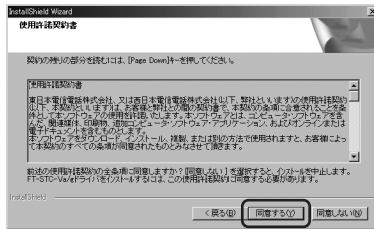
お知らせ

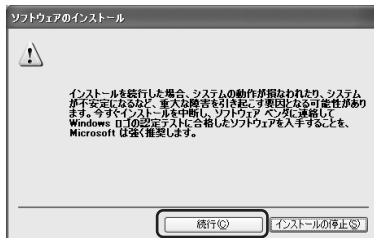
- この時点では、無線LANカード本体をPCカードスロットに挿入しないでください。パソコンの電源をONにする前、もしくはOSが起動した時点で本商品を挿入した場合、ドライバのインストールに失敗する恐れがあります。

2 CD-ROMドライブに付属のCD-ROMをセットすると、次のメニュー画面が自動的に起動します。

起動したら、「ドライバとユーティリティのインストール」をクリックします。
ダウンロード確認画面が表示される場合があります。その際は、「開く」をクリックしてください。

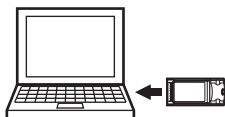
3 インストール確認画面が開きます。「次へ」をクリックします。

4 使用許諾契約書の画面が開きます。
内容を確認の上、よろしければ「同意する」をクリックします。

5 インストール先の選択画面が開きます。
ドライバのインストール先を変更される場合は「参照...」をクリックして、インストール先を指定します。変更の必要がなければ、「次へ」をクリックします。

6 以下のような確認メッセージが出ます。
「続行」をクリックしてインストールを継続します。

(次ページに続く)

本商品とパソコンの設定

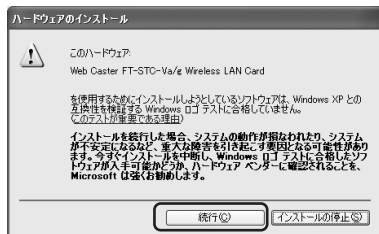
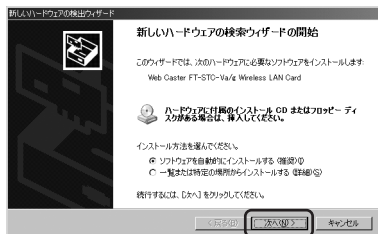
7 インストールが完了するとセットアップの完了画面が表示されます。「完了」をクリックしてください。その後、P3-14手順2で表示されている画面下の「END」をクリックしてください。

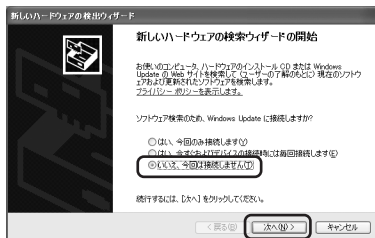
8 無線LANカード本体のランプが見える側を上にして、PCカードスロットの奥まで挿入します。

お知らせ

- PCカードスロットの位置・使用方法については、お使いのパソコンにより異なります。わからない場合にはパソコンの取扱説明書等をご覧ください。

※無線LANカードが正しく認識されると、メッセージが表示される場合があります。

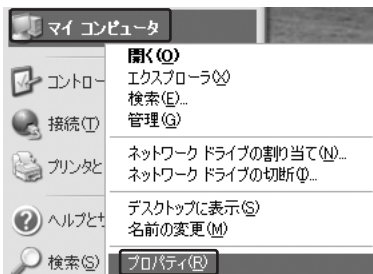
※次ページ手順9の画面が先に表示される場合もあります。

9 左下のような「新しいハードウェアの検索ウィザード」画面が表示されますので、そのまま「次へ」をクリックしてください。無線LANカードが正しく認識されると、右下のような確認メッセージが出ます。「続行」をクリックの後、表示される画面で「完了」をクリックするとインストールが完了します。

お知らせ

● ご使用のパソコンにWindows® XP ServicePack2をインストールしている場合、「新しいハードウェアの検索ウィザードの開始」画面は以下のイメージで表示されます。[いいえ、今回は接続しません] を選択した後、「次へ」をクリックしてください。このあと、手順9の右側の画面が表示されますので、手順9の内容に従って進めてください。

以上でインストール作業は完了しました。
メニューを終了してから、次ページの「⑥インストールの状態を確認する」にお進みください。

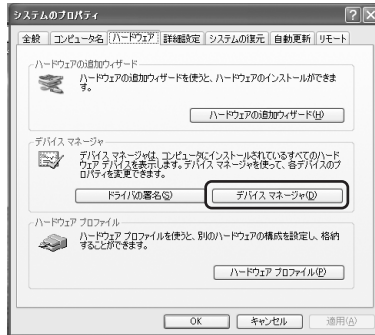
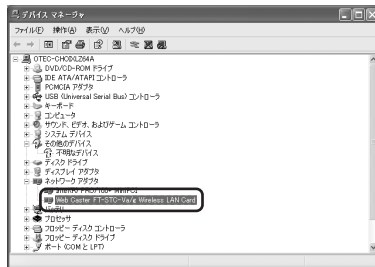
本商品とパソコンの設定

⑥インストールの状態を確認する

1 「スタート」ボタンをクリックし、「マイコンピュータ」上で右クリックして「プロパティ」をクリックします。

お知らせ

● Windows® XP以外のOSをお使いの場合は、「マイコンピュータ」のアイコンはデスクトップ上にあります。

2 「システムのプロパティ」の画面上の「ハードウェア」タブをクリックします。

3 デバイスマネージャの項の「デバイスマネージャ」をクリックします。

4 「デバイスマネージャ」の「ネットワーク　アダプタ」をダブルクリックし、「Web Caster FT-STC-Va/g Wireless LAN Card」があることを確認します。

お知らせ

- 「Web Caster FT-STC-Va/g Wireless LAN Card」のアイコンの前に“！”マークがついている場合は、何らかの問題が発生しています。
  その際には、パソコンの再起動をするか、ドライバの再インストールを行ってください。

本商品とパソコンの設定

⑦パソコンからアクセスポイント（本商品）へ通信する（インフラストラクチャ・モード）

インフラストラクチャ・モードとは、無線LANカードを装着したパソコンからアクセスポイントを介し、無線LAN上で通信を行う場合に設定するモードです。
ここでは、無線LANカードを装着したパソコンから、アクセスポイント（本商品）に無線LANで接続するための設定をします。

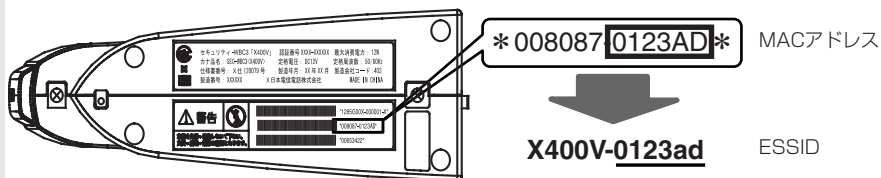
1 本商品の電源が入っていることを確認します。

2 本商品のESSID（ネットワーク名）を確認します。

本商品のESSID（ネットワーク名）を記録しておいてください。

※本商品のESSIDについては、工場出荷時に「X400V-【MACアドレスの下6桁（英数小文字）】」で設定されています。

●MACアドレスの確認方法

本体底面にシールが2箇所貼り付けてあり、バーコードがあるシールにMACアドレスが記載してあります。
中央のバーコードの右に書いてあるものがMACアドレスになります。

［本商品の底面］

シールの表示が上記の場合は、本商品のESSIDは「X400V-0123ad」となります。
※ESSIDの「X400V-」のアルファベットは大文字、「0123ad」のアルファベットは小文字となりますのでご注意ください。

お知らせ

● ESSIDとは、本商品と無線LANアクセスポイントとが通信時に使用するネットワーク識別用のIDです。無線LANアクセスポイントにESSIDを設定しておき、その無線LANアクセスポイントと接続するパソコン等にも同じSSIDを設定しておけば、通信が可能になります。このように、接続する無線LANアクセスポイントをESSIDで指定することができます。ESSIDは、セキュリティ機能の一つに分類される場合もありますが、あくまでも接続先の識別機能ですので、ESSIDを設定後に、他のセキュリティ設定をすることをお勧めします。

この時点で、ドライバのインストールが完了し、カードがPCカードスロットに挿入されているものとします。
カードのPOWERランプが点滅していることを確認してください。

3 タスクトレイのユーティリティアイコン をダブルクリックします。

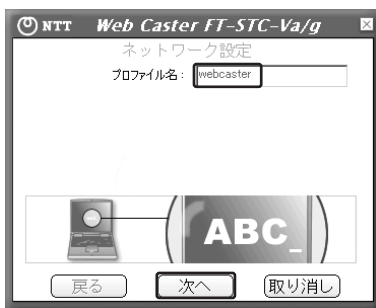
アイコンが表示されていない場合は、[スタート]ボタン→[すべてのプログラム]→[WBC FT-STC-Vag]→[FT-STC-Vag設定ユーティリティ]をクリックしてください。

4 ユーティリティの画面が開きます。

（次ページに続く）

本商品とパソコンの設定

5 上部の［設定］タブをクリックします。工場出荷時は何も入っていませんので、［追加］をクリックしてネットワーク設定を行います。

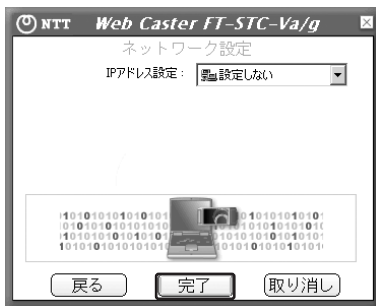
6 ネットワーク設定を行います。プロファイル名は任意の英数字を入力してください。入力が完了したら［次へ］をクリックしてください。

7 **事前に調べておいたアクセスポイント（本商品）のネットワーク名（ESSID）をSSIDの欄に入力します。**

入力が完了したら［次へ］をクリックしてください。

8 **［次へ］をクリックしてください。**

アクセスポイント（本商品）が暗号化されている場合は、後述の「⑧無線LANカードに暗号化を設定する」に従って認証モードを変更してください。

（次ページに続く）

本商品とパソコンの設定

9 [完了]をクリックしてください。

お知らせ

● 本ユーティリティを使用してIPアドレスを設定する場合はIPアドレス設定メニューから[設定する]を選択した後、[次へ]ボタンをクリックしてIPアドレス入力画面で設定を変更してください。

10 設定した内容が反映されることを確認してください。リストから追加したネットワーク設定を選択した状態で、[接続]をクリックしてください。

通信をしているネットワーク名の前には 印がつきます。

11 手順10で表示されている画面上部の［設定選択］タブをクリックし、［詳細…］をクリックします。詳細情報が表示されますので［無線LAN情報］の信号強度と通信品質が表示されていることを確認した後、ウィンドウを閉じます。

以上で、アクセスポイント（本商品）との無線LAN接続関連の設定は終了です。
通信内容の暗号化設定を行う場合は、引き続き「⑧無線LANカードに暗号化を設定する」をお読みください。

お知らせ

● タスクトレイに格納されているアイコンを確認することでも通信状態を確認することができます。

- ：　無線LANネットワークに接続中
- ：　無線LANネットワークを検索中

本商品とパソコンの設定

⑧無線LANカードに暗号化を設定する

無線LANカードに暗号化を設定します。
ここではアクセスポイント（本商品）に暗号化方式WPA-PSK、入力方式TKIP、ネットワークキー「abcdefgh」を設定したときの設定例を示します。
「TKIP」を使用しない場合は、「Web Caster FT-STC-Va/g」や「Web Caster FT-STC-Oa/g」のマニュアルを参照してください。
この時点で、ドライバのインストールが完了し、カードがPCカードスロットに挿入されているものとします。
カードのPOWERランプが点滅していることを確認してください。

お知らせ

- 暗号化方式でWPAを使用するには、Windows® XPサービスパック1以上とWPAサポート修正プログラムをあらかじめインストールしておく必要があります。本書は上記サービスパックおよび修正プログラムがご使用のパソコンにインストールされていることを前提に記述しています。
- WPAサポート修正プログラムについてはマイクロソフト社のサポート技術情報 826942「Windows XP の WPA ワイヤレス セキュリティ アップデートの概要」を参照してください。マイクロソフト社のホームページ（http://www.microsoft.com/japan/）で、「サイトの検索」欄に 826942 と入力し、「検索」をクリックすることで参照できます。

1 タスクトレイのユーティリティアイコン をダブルクリックします。

アイコンが表示されていない場合は、[スタート]ボタン→[すべてのプログラム]→[WBC FT-STC-Vag]→[FT-STC-Vag設定ユーティリティ]をクリックしてください。

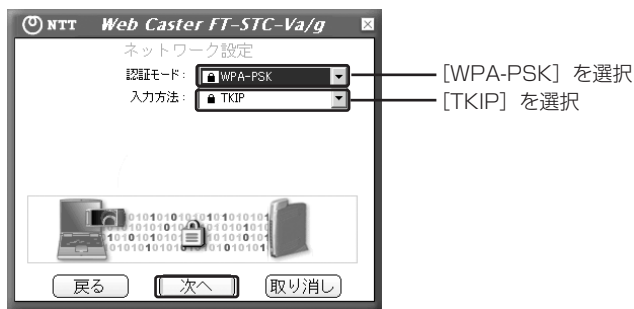
2 ユーティリティの画面が開きます。

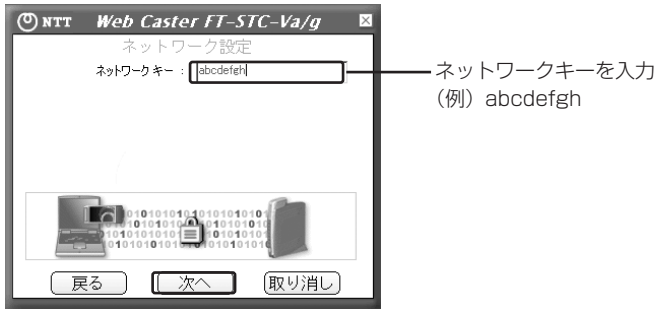
3 上部の[設定]タブをクリックします。利用するネットワーク設定を選択し、[変更]をクリックします。

（次ページに続く）

本商品とパソコンの設定

4 ［プロファイル名］の設定画面が表示されますので［次へ］をクリックして［認証モード］の設定画面まで進みます。

5 [認証モード]のメニューから[WPA-PSK]を選択し、[入力方法]メニューから[TKIP]を選択し、[次へ]をクリックします。

6 アクセスポイント（本商品）で設定したネットワークキー（事前共有キー）を入力してください。

入力が完了したら［次へ］をクリックしてください。

7 IPアドレス設定の画面が表示されますので［完了］をクリックしてください。

以上で、暗号化の設定は終了です。

本商品とパソコンの設定

⑨無線LAN接続を確認する

パソコンと本商品を接続していたLANケーブルを抜いて、Webブラウザで本商品にログインできるかお試しください。通信できない場合は手順にそって設定内容をご確認ください。

⑩必要に応じて本商品と無線LANカードの設定を変更する

これまでの手順で無線LANに関する基本的な設定は完了しています。お客様のご使用方法に応じて設定の変更が必要な場合は、ここで変更を行ってください。（「無線LAN設定」（☛P2-35）、「無線LANカード取扱説明書」、「詳細取扱説明書」参照）

⑪無線LAN設定を終了する

以上の手順を実施していただくと、本商品を無線LANのアクセスポイントとして使用することが可能になります。

LANケーブルを使用しない設定

これまで、パソコンと本商品をLANケーブルで接続して本商品と無線LANカードを設定する基本的な方法を説明しましたが、LANケーブルを使用しないで設定する場合は以下の手順で本商品と無線LANカードの無線LAN設定を実施することができます。

本商品の設定

無線LANカードの設定

②本商品に無線LAN カードを装着する （☛P3-5）

↓

⑤パソコンに無線LAN カードのドライバをインストールする（☛P3-13）

↓

⑥インストールの状態を確認する （☛P3-18）

↓

⑦パソコンからアクセスポイント（本商品）へ通信する（インフラストラクチャ・モード） （☛P3-20）

↓

③本商品に暗号化を設定する （☛P3-6）

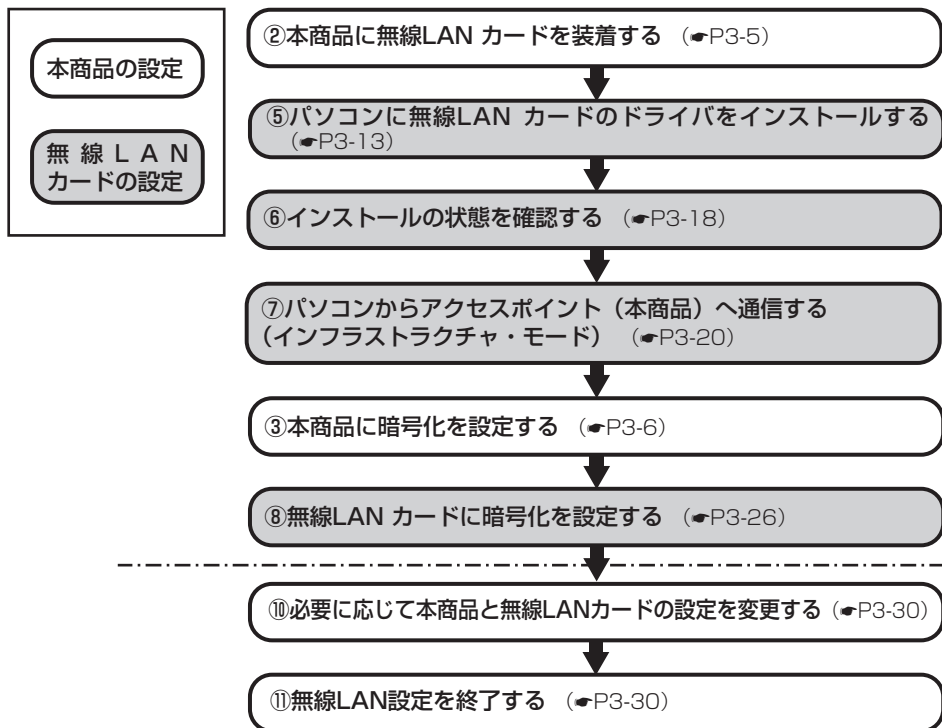
↓

⑧無線LAN カードに暗号化を設定する （☛P3-26）

↓

⑩必要に応じて本商品と無線LANカードの設定を変更する（☛P3-30）

↓

⑪無線LAN設定を終了する （☛P3-30）

お知らせ

● Webブラウザで本商品にログインし、本商品の設定を変更してから再起動すると、その後すぐには無線LANカードを装着したパソコンからWebブラウザで本商品にログインできず、「ページが表示できません」の画面になる場合があります。

4 お困りのときには

本商品がうまく動かない、操作しても違う結果になるなど、お困りのときにはこちらをお読みください。

トラブルや疑問点がある場合 ･････････4-2

トラブルや疑問点がある場合

本商品がうまく動かない、操作しても違う結果になるなど、お困りのときにはこちらをお読みください。
該当項目がない場合や、対処をしても問題が解決しない場合は、本商品を初期化して、初めから設定し直してください。初期化を行うと本商品のすべての設定が消去されますのでご注意ください。初期化を行う場合は現在の設定内容をお手元に記録しておくことをお勧めします。（取扱説明書「本商品の初期化について」）

設定に関するトラブル

症　状	原因と対策
PPPランプが消灯している (オフライン中)	①「PPPoE設定」画面の「セッション設定」にて「使用するセッション」に設定した「接続先1〜5」の「接続ユーザ名」、「接続パスワード」、「無通信監視タイマ」が正しい内容であるか確認してください。（「PPPoE設定」（☛P2-11）） ②「状態表示2」画面で「PPPoE状態」を確認してください。「接続先1〜5」が全て「未使用」になっている場合は、全ての接続先が「切断」状態になっています。「接続先1〜5」が全て「異常」「認証エラー」の状態になっている場合も、全ての接続先が「切断」状態になっています。使用する「接続先」に対して「接続」を行ってください。（「状態表示2」（☛P2-51）） ③ 本商品とADSL/VDSLモデム、回線終端装置等の接続構成および、本商品背面のWAN側接続ポート等、ケーブルの種類や接続状態を再度ご確認ください。（取扱説明書「回線を接続する」） ※①〜③で改善しない場合は、6分〜10分程度そのままお待ちください。お待ちになってもPPPランプが緑点灯しない場合は当社、お問い合わせ先窓口へお問い合わせください。
VoIPランプが消灯している (IP電話回線利用不可)	① IP電話の設定が正しくできていません。「IP電話の設定」を再度実施してください。 ② IP電話サービスが「無効」（利用停止）に設定しているか確認してください。「無効」となっている場合は「有効」に変更してください。（「サービス設定」（☛P2-43）、「機能仕様」（☛P5-4））

通話/ダイヤルに関するトラブル

症　状	原因と対策
ハンドセット（受話器）を取り上げても発信音が聞こえない	本商品と電話機を接続している電話機コードを含め機器の接続構成を確認してください。（取扱説明書「回線を接続する」）
電話機からダイヤルしても発信音が停止しない	① 電話機の設定が加入電話回線契約（DP（ダイヤルパルス指定）／PB（プッシュボタン信号指定））と一致しているか確認してください。一致していないときは電話機の設定を変更してください。 ②「加入電話回線種別」が加入電話回線の契約と一致しているか確認してください。一致していない場合は、「加入電話回線種別」を変更してください。 （「サービス設定」（☛P2-43））
相手先が応答しない	① 相手先の電話番号を確認してください。 ②「市外局番」が正しい番号か確認してください。間違っている場合はIP電話の設定をやり直してください。 （取扱説明書「IP電話の設定」） ③呼出中音や話中音が聞こえない場合は、相手先番号が誤っている可能性があります。電話番号を確認してください。 ④ダイヤル中に停電などで本商品の電源が切れた可能性があります。電源を入れたあと再度ダイヤルしてください。
IP電話回線が利用できない （「VoIP」ランプが点滅しない）	① 加入電話回線を選択する電話番号をダイヤルしている場合があります。（TELランプが橙点滅します。）電話番号をご確認ください。（取扱説明書「加入電話回線を選択する電話番号」、「加入電話選択発信」（☛ P5-3）、「加入電話自動迂回」（☛P5-4）） ② 緊急通報(110/118/119)にダイヤルした場合は本商品側の電話機がハンドセット（受話器）を置いても通話は終了しません。（相手先が通話を終了するまで継続します。）緊急通報が終了するまでお待ちください。 ③ 本商品がIP電話サービスをご利用いただけない状態になっている可能性があります。本商品の電源を入れ直してください。
特定の相手先からの電話がかかってこない	相手先を着信拒否登録していないか確認してください。登録されている場合は解除を行ってください。（「サービス設定」（☛P2-43）、「機能仕様」（☛P5-3））

トラブルや疑問点がある場合

パソコンに関するトラブル

症　状	原因と対策
パソコンからインターネットへアクセスできない	① 使用する接続先の「接続ユーザ名」、「接続パスワード」、「無通信監視タイマ」が正しい内容であるか確認してください。（「PPPoE設定」（☛P2-11）） ②「状態表示2」画面で「PPPoE状態」を確認してください。 ・使用する接続先が「未使用」になっている場合は、「切断」状態になっています。使用する「接続先」に対して「無通信監視タイマ」が「無効」に設定されている場合は「接続」を行ってください。 ・「異常」「認証エラー」の状態になっている場合も接続先が「切断」状態になっています。「接続」を行ってください。（「状態表示2」（☛P2-51）） ③ 本商品とADSL/VDSLモデム、回線終端装置等の接続構成および、本商品背面のWAN側接続ポート等、ケーブルの種類や接続状態を再度ご確認ください。（取扱説明書「回線を接続する」） ④ パソコンにIPアドレスが設定されているか確認してください。（取扱説明書「パソコンを設定する」および「パソコンのネットワーク設定」） ⑤ 本商品からパソコン側にPingを送信し通信の正常性を確認してください。（「Ping送信」（☛P2-63）） ⑥ ブラウザやARPのキャッシュ情報をクリアするためにパソコンの再起動を実施してください。 ⑦ パソコンを再起動してください。その後、「状態表示１」をクリックします。 ・「更新確認」をクリックし、セキュリティバージョンの「現在のバージョン」と「最新のバージョン」が一致していることを確認してください。一致していない場合は「ダウンロード実行」をクリックし、ファームウェア手動アップデートを実行してください。 ・セキュリティバージョンの「アップデート状態」がすでに、「プログラムの更新中です。」と表示されている場合は数分後に再度「状態表示１」をクリックし、プログラム更新が終わったこと（「新しい更新はありません。」が表示されます。）を確認のうえ使用してください。（取扱説明書「バージョンアップ方法（「状態表示１」画面）」および「状態表示１」（☛P2-48））

症　状	原因と対策
パソコンからインターネットへアクセスできない	⑧ 自動バージョンアップによるファームウェア更新中か確認してください。（ALARM、PPP、VoIP、TELランプが同時にゆっくりと点滅します。）　更新中の場合は、更新が終了することを確認のうえ使用してください。（取扱説明書「自動バージョンアップアップ機能を利用してバージョンアップする」） ※①～⑧で改善しない場合は、6分～10分程度そのままお待ちください。お待ちになってもPPPランプが緑点灯しない場合は当社、お問い合わせ先窓口へお問い合わせください。
パソコンからインターネットへアクセスできない（WANランプが消灯している）	本商品とADSL/VDSLモデム、回線終端装置等との接続構成および接続しているLANケーブルの種類を確認してください。（取扱説明書「回線を接続する」）
パソコンを接続したLAN側接続ポートのLINKランプが消灯している	① 本商品とパソコン等との接続構成および接続しているLANケーブルの種類を確認してください。（取扱説明書「回線を接続する」） ② 接続に問題がなければ、LANカードが正しく動作しているか確認してください。なお、LANカードについてのトラブルは、パソコンあるいはLANカードのメーカーにご相談ください。
Webブラウザで本商品にログインできない	●ユーザー名/パスワードが誤っていませんか？ ・正しいユーザー名/パスワードを入力してください。 ・ユーザー名：admin ・パスワード：初期設定で入力したもの（取扱説明書「かんたん設定」） ※パスワードは忘れないようにメモして安全な場所に保管してください。お忘れになった場合は、本商品を初期化してください。（取扱説明書「本商品の初期化について」）パスワードを変更したときは「反映」を必ずクリックしてください。忘れると、再起動したあとや本商品の電源を入れ直したあとに元のパスワードへ戻ってしまいます。
Webブラウザで変更した通りに動作しない	●Webブラウザで本商品の設定変更後、「反映」をクリックしましたか？ ・「反映」をクリックしてください。 ●Webブラウザは適切なバージョンがパソコンにインストールされていますか？ ・インストールをされていない場合には雑誌の付録CD-ROM等からインストールを行ってください。また、インターネット環境がすでにある場合は、マイクロソフト社のホームページからダウンロードをすることも可能です。

トラブルや疑問点がある場合

ウイルス／不正アクセスに関するトラブル

症　状	原因と対策
ウイルス検出（VIRUSランプ：赤点灯）したが、元の状態（緑点灯）への戻し方が分からない	Webブラウザ設定画面のメニューから「ログ表示」をクリックして表示されるサブメニューから「ウイルスログ表示」をクリックします。 ウイルスが検出されたことを示すログを確認してください。ウイルスログ表示画面を見ることでVIRUSランプはウイルス検出前のランプ状態に戻ります。（「ウイルスログ表示」（☛P2-59））
不正アクセス検出（HACKERランプ：赤点灯）したが、元の状態（緑点灯）への戻し方が分からない	Webブラウザ設定画面のメニューから「ログ表示」をクリックして表示されるサブメニューから「不正アクセスログ表示」をクリックします。不正アクセスが検出されたことを示すログを確認してください。「不正アクセスログ表示」画面を見ることでHACKERランプは不正アクセス検出前のランプ状態に戻ります。（「不正アクセスログ表示」（☛P2-59））
MSN ExplorerでWebメールを使用している場合、Webメールの添付ファイルからウイルスを検索することができますか？	MSN Explorerをご使用の場合、本商品でWebメールの添付ファイルを検索することはできません。これは、MSN ExplorerではWebメールの受信に異なるプロトコルを使用しているためです。Internet Explorerのご使用をお勧めします。
Internet Explorerでウイルス駆除できなかったWebメールの添付ファイルやファイルサイズが4MB以上の添付ファイルを保存するにはどうしたらよいですか？	ウイルス駆除できなかったWebメールの添付ファイルや4MB以上のWebメールの添付ファイルを保存するには、本商品のWebメールのウイルス検索機能を無効にする必要があります。ただし、Webメールのウイルス検索を無効にすると、Webメールの添付ファイルに対してウイルス検索が実行されません。 また、Webメールが有効になっているときに、添付ファイルを右クリックし［別名で保存］を選択しても保存できませんので、ご注意ください。
Outlook ExpressでHotmailメッセージを受信するように設定している場合、本商品ではHotmailの添付ファイルに対してウイルス検索を実行できますか？	できません。Outlook ExpressでHotmailを受信するように設定している場合、本商品ではそのHotmailに対してウイルス検索を実行することができません。Hotmailの添付ファイルに対してウイルス検索が実行されていないことも通知されません。これはOutlook Expressでは、Hotmailメッセージの受信に異なるポートを使用しているためです。ウイルスに感染しないようにするためにも、Hotmailの受信にはWebブラウザをお使いいただくことをお勧めします。

症　状	原因と対策
POP3、SMTP、HTTPは通常、ポート番号110、25、80にそれぞれ割り当てられています。このプロトコルに別のポートを割り当てた場合、本商品では送受信e-mailおよびWebメールに対してウイルス検索を実行することはできますか？	できません。POP3、SMTP、HTTPに別のポートを割り当てた場合、本商品では送受信e-mailおよびWebメールに対してウイルス検索を実行することができなくなります。また、送受信e-mailおよびWebメールに対してウイルス検索が実行されていないことも通知されません。
ウイルスに感染したファイルをダウンロードしようとした場合、本商品はこのウイルスを発見してくれるのでしょうか？	ダウンロードするファイルに対して、リアルタイムでウイルス検索は実行しません。 ダウンロード後、オンラインウイルス検索機能で検索、駆除することが可能です。
ウイルス対策の対象は何ですか？	ウイルス検索の対象は、送信メール（SMTP）と受信メール（POP3）およびWebメールの添付ファイルとなります。 対応しているWebメールは、Yahoo!メール、Hotmail、AOLメールです。
メールのウイルス検索の制限はありますか？	下記の条件を満たしているファイルは、ウイルス検索可能です。 ・ 添付ファイルを含めて4MByte以内のサイズのメール（メールヘッダ、本文を含みます。圧縮ファイルの場合は解凍後のサイズ、また添付ファイルが複数の場合はその合計サイズ。） ・暗号化されていないメール ・パスワード保護されていないファイル ・2回以内の圧縮ファイル ・ヘッダを改ざんしていないメール この制限を超えたメールを処理した場合は、ウイルス検索が実行されていない旨の通知がメールに添付されます。（取扱説明書「セキュリティに関するご注意」）
メールの添付ファイルのエンコード形式は何をサポートしていますか？	エンコード形式としては、次の形式をサポートしています。 ・Quoted Printable ・base64 ・Uuencode ・7-bit ・8-bit ・binary TNEF ・Plain Text （取扱説明書「セキュリティに関するご注意」）

（次ページに続く）

トラブルや疑問点がある場合

症　状	原因と対策
オンラインウイルス検索はどうやって行うのですか？	オンラインウイルス検索をお使いになる場合、本商品設定画面から起動します。 Webブラウザで本商品にログインし、画面左下の「オンラインウイルス検索」アイコンをクリックすると使い方が表示されます。 内容をよく読んだ上で、ご利用ください。 ※「オンラインウイルス検索」アイコンは、フレッツ・セーフティの利用登録がお済みの方のみに表示されます。 <動作制限事項> ・OS：Windows® XP/Me/98以上、Windows® 2000 Professional オンラインウイルス検索は、Mac OSには対応していません。 ・ソフトウェア：Internet Explorer 5.5 サービスパック2以上 ・CPU：386 DX（486 DX以上推奨） ・RAM：4MB（8MB以上推奨） ・ハードディスク：10MB以上のディスク空き容量 ・ActiveXコントロールのダウンロード画面が表示される場合があります。 ・Internet ExplorerでActiveXコントロールを有効にしてください。「ツール」メニューの「インターネットオプション」をクリックし、「セキュリティ」タブの「レベルのカスタマイズ」をクリックし、有効になっているかを確認してください。（取扱説明書「オンラインウイルス検索」）（2005年10月現在の情報です。） ・フレッツ・セーフティをご契約いただいていない場合は、オンラインウイルス検索の一部の機能はご利用になれません。 ・オンラインウイルス検索の動作や内容に関しては、フレッツ・セーフティサービス、および本商品のサポート対象外となります。
本商品を導入すればウイルスバスター等のウイルス対策ソフトは不要になりますか？	本商品は、メールのウイルス検索とファイアウォール機能を持っています。これらのみの用途であれば、フレッツ・セーフティだけで十分ウイルス対策はできます。 ウイルス対策ソフトと併用していただいても問題はありません。ただし、市販ソフトのパーソナルファイアウォールなど、フレッツ・セーフティと重複する機能については、無効にしていただくことをお勧めします。
Web閲覧時にもウイルス検索を行いますか？	本商品は、Web閲覧時などのHTTP経由、FTP経由でのウイルスに関しては検出を行いません。 しかし、本商品のオンラインウイルス検索を利用することでダウンロードしたファイルのウイルス検出、駆除が可能となります。また、リアルタイムで感染を防止する場合はコンピュータにインストールするタイプのウイルス対策ソフトを導入し、二重にセキュリティ対策を行ってください。

無線LANに関するトラブル

症　状		原因と対策
無線LANクライアント（無線LANカードを装着したパソコン）からインターネットに接続できない	無線LAN通信ができる	本商品のWAN側の設定を確認してください。（取扱説明書「かんたん設定」）
	無線LAN通信ができない（本商品に装着している無線LANカードのPOWERランプが消灯している）	本商品側の無線LANカードが正しく装着されていることを確認してください。 ・本商品のカードスロットの奥まで正しく無線LANカードが挿入されていることを確認してください。
	無線LAN通信ができない（本商品に装着している無線LANカードのPOWERランプおよびLINKランプが点滅している）	①パソコン側の無線LANカードが正しく装着されていることを確認してください。 ・パソコンのPCカードスロットの奥まで正しく無線LANカードが挿入されていることを確認してください。 ・パソコンにPCカードスロットが複数ある場合には、他のPCカードスロットに差し替えてみてください。 ②設置場所を変えてください。 ・本商品とパソコンを壁から離してください。 ・パソコンを見通せる位置に本商品を設置してください。 ・本商品とパソコンをディスプレイや他のパソコンの近くには設置しないでください。（パソコンから信号強度、接続品質などを確認してください。） ③本商品とパソコンの設定を確認してください。（暗号化、ESSIDなど。）（「無線LANを利用する」（☛P3-11）） ④パソコンのIPアドレスを確認してください。（ipconfigコマンドなど）IPアドレスが正しく設定されていないときは、パソコンのIPアドレスの取得方法と本商品のDHCP設定に不一致がないか確認してください。 ⑤通信に使用しているチャネルや動作モードを変更してください。（「無線LANを利用する」の「④本商品の無線LAN設定を確認する」（☛P3-11）） ・11bまたは11gを使用している場合は11aに変更してください。
11gを使用しているのにスループットが低下した		11gと11bを混在して使用している場合は、11b+gモードにしてください。（「無線LANを利用する」の「④本商品の無線LAN設定を確認する」（☛P3-11））

※パソコン側の無線LANカードに関するトラブルは無線LANカードの「取扱説明書」「詳細取扱説明書」を参照してください。

トラブルや疑問点がある場合

バージョンアップに関するトラブル

症　状	原因と対策
「アップデートの状態」に「更新の確認に失敗しました。」と表示される	● PPPランプが消灯していませんか。 →PPPoE接続が切断されています。接続後、「状態表示1」画面の「更新確認」をクリックしてください。(「状態表示1」(☛P2-48)) ● 自動アップデート用のURLが間違っていませんか。 →「IP電話設定情報」の「アップデート確認用URL」を確認してください。(「IP電話設定情報」(☛P2-46))
ハンドセット（受話器）を取り上げると「ピーピーピーピー」と音がする	最新のプログラムがあることを通知しています。プログラムの更新を行ってください。正常動作です。(取扱説明書「バージョンアップお知らせ機能を利用してバージョンアップする」)
「アップデートの状態」に「ファームウェアのダウンロードに失敗しました。」と表示される	● PPPランプが消灯していませんか。 →PPPoE接続が切断されています。接続後、「状態表示1」画面の「更新確認」をクリックし、更新された「アップデート状態」の表示内容にしたがって作業を行ってください。(取扱説明書「バージョンアップ方法（「状態表示1」画面)」)
設定画面から「ダウンロード実行」をクリックしても、ダウンロードが始まらない また、「自動アップデート」の「実行時刻」になってもダウンロードが始まらない	● 通話中ではありませんか。 →通話終了後に自動的にダウンロードが開始されます。(取扱説明書「バージョンアップ方法（「状態表示1」画面)」)
「アップデートの状態」に「ファームウェアの更新に失敗しました。」と表示される	●PPPランプが消灯していませんか。 →PPPoE接続が切断されています。接続後、「状態表示1」画面の「更新確認」をクリックし、更新された「アップデート状態」の表示内容にしたがってバージョンアップを行ってください。(取扱説明書「バージョンアップ方法（「状態表示1」画面)」)
Mac OSのパソコンからバージョンアップができない	プログラムをダウンロードするときに、拡張子をbinからfooなどの任意の文字に変更してから保存してください。
自動バージョンアップができない	●「自動アップデート」の「実行時刻」を確認してください。(取扱説明書「自動バージョンアップ機能を利用してバージョンアップする」) ●本商品の電源を落とさずにご利用ください。電源が切れているとファームウェアの更新ができない場合があります。(取扱説明書「自動バージョンアップ機能を利用してバージョンアップする」)

その他のトラブル

症　状	原因と対策
電源アダプタを電源コンセントに差し込んだのに本商品のPOWERランプが緑点灯しない	アダプタのケーブルが本商品に接続されているか確認してください。
ALARMランプが点灯する	本商品で異常が発生しています。本商品の電源を入れ直しても改善しない場合は、当社、お問い合わせ先窓口へお問い合わせください。
ALARMランプが点滅する	本商品で異常が発生しています。初期化をして設定データを再度登録し直してください。改善しない場合は、当社、お問い合わせ先窓口へお問い合わせください。（取扱説明書「本商品の初期化について」）
●ログ表示の日時が1970年代になっている ●「ソフトウェアアップデート」および「ハッカーの不正アクセス」通知のメールの日付が1970年代になっている ●「日時情報の合わせ方」がわからない	本商品に誤った「ＮＴＰサーバアドレス」が設定されています。もう一度設定をやり直してください。 （取扱説明書「時刻の設定について」）
ALARM、PPP、VoIP、TELランプが遅い点滅をしている	バージョンアップを実行中です。PPPランプが緑点灯（2セッション以上接続時は橙点灯）するまで電源を切らずにお待ちください。
ALARM、PPP、VoIP、TELランプが速い点滅をしている	異常が発生しました。当社、お問い合わせ先窓口へお問い合わせください。
ファームウェア更新や「反映」、「初期設定へ戻す」、「再起動」クリックなどにより、システム更新後または再起動後に「かんたん設定」画面が表示されない（「ページを表示できません」画面が表示される）	ALARMランプ以外が点灯したことを確認してください。次にコマンドプロンプトから半角英数字で「ipconfig /renew」と入力するなどして、パソコンに設定されているネットワーク情報を更新したあと、webブラウザのアドレスバーに「http://192.168.1.1/」と入力して再度接続を試みてください。

(注) 上記対策を実施しても問題が解決しない場合、上記問題以外のトラブルが発生した場合は、当社、お問い合わせ先窓口へお問い合わせください。

5 付録

機能仕様 ··························5-2
用語集 ····························5-12
索引 ······························5-25
設定記入シート ······················5-27

機能仕様

電話機能

サービス機能	内　容	Web画面
発信時の基本動作	相手に電話をかけて通話することができます。（取扱説明書「電話をかける（発信）」）	
着信時の基本動作	相手からの電話を受けて通話することができます。（取扱説明書「電話を受ける（着信）」）	
話中時などの動作	相手が話中などで電話がつながらない場合は、つながらないことが音で通知されます。（取扱説明書「相手がお話し中のとき」）	
電話番号による回線選択	通常はIP電話サービスをご利用になれますが、一部IP電話サービスをご利用できない電話番号（従来の加入電話回線をご利用いただくことになります。）や発信を制限している電話番号があります。（取扱説明書「加入電話回線を選択する電話番号」、および「加入電話自動迂回」（☛P5-4）） （注）停電中、装置障害中（本商品のALARMランプが赤点灯/点滅）の場合はIP電話サービスをご利用できません。	
お話し中にかかってきた電話を受けるには（キャッチホン）	お話し中でもかかってきた電話に出ることができます。（取扱説明書「お話し中にかかってきた電話に出る」）	サービス設定（[利用中電話サービス] キャッチホン・[IP電話サービス] 割り込み音）
緊急通報（110/118/119）	緊急時は110/118/119をダイヤルし警察/海上保安/消防へ連絡することができます。 （注）ハンドセット（受話器）を置いてもしばらくIP電話サービスをご利用できない場合があります。	
発信者番号通知/拒否ダイヤル（184/186）発信	相手先番号の前に184/186をダイヤルすることで相手に自分の電話番号を通知する/しないを指定することができます。（取扱説明書「発信者番号の通知と表示」）	サービス設定（[IP電話サービス] 発信時番号通知）
ナンバー・ディスプレイ	電話がかかってきたときの相手先電話番号が電話機のディスプレイに表示されます。（取扱説明書「かけてきた相手の電話番号を表示するには（ナンバー・ディスプレイ）」） （注）ナンバー・ディスプレイ対応の電話機が必要になります。	サービス設定（[利用中電話サービス] ナンバー・ディスプレイ）

サービス機能	内　容	Web画面
着信拒否	迷惑電話などを防止するため、IP電話サービス電話番号に着信した場合、相手からの呼び出しを次回以降拒否することができます。 (1) 登録方法 ①通話終了後、ハンドセット（受話器）を取りあげ「＊＊＊02」をダイヤルしてください。 ②ダイヤルが終了すると「ププ」という音が聞こえますのでハンドセット（受話器）を置いてください。それで登録が終了です。 ・登録は最大30件まで可能です。30件以上登録した場合は古い方から削除されます。 (2) 解除方法 ①ハンドセット（受話器）を取りあげ「＊＊＊03」をダイヤルしてください。 ②ダイヤルが終了すると「ププ」という音が聞こえますのでハンドセット（受話器）を置いてください。それで解除が終了です。 ・登録したダイヤルはすべて解除されます。個々のダイヤルの解除はできません。個々のダイヤルの解除は、Web設定画面で行ってください。「サービス設定」（☛P2-43） ※プッシュホン信号を送出できる電話機をご使用ください。（信号種別を変更できる電話機をご使用の場合は、「PB」に切り替えればご使用になれます。） ※従来の加入電話回線に対し着信拒否を行いたい場合は「迷惑電話おことわりサービス」（有料）をご契約ください。	サービス設定 ([IP電話サービス] IP電話　着信拒否 電話番号)
ファクス通信	相手とファクスの送信/受信ができます。 （注）ファクス通信中に割り込み音が入ると通信が切断されます。確実にファクス通信を行いたい場合は、サービス設定で「割り込み音」を「なし」に設定してください。	
プッシュホン信号による各種サービス対応	プッシュホン電話機からダイヤルをすることで留守番電話機のサービスなど各種サービスを受けることができます。	
加入電話選択発信	加入電話を選択して発信したいときは「0000」をダイヤルしてから相手番号をダイヤルします。 （注）このときの通話料金はお客様が契約されている電話会社からの請求となります。	

（次ページに続く）

機能仕様

サービス機能	内　容	Web画面
Lモード	Lモードサービスがご利用になれます。 （注）Lモードの契約、Lモード対応電話機が必要になります。 ご使用の電話機によっては正常に通信できない可能性があります。	サービス設定 （[利用中電話サービス]ナンバー・ディスプレイ）
加入電話自動迂回	IP電話サービス提供外の番号へダイヤルしたときは自動的に加入電話へ再発信されます。そのとき「ププププ」という断続音のあとに「プー」という音が聞こえます。	
IP電話サービス利用停止	IP電話サービスのご利用を規制します。（無条件で加入電話回線を選択します。）お客様が一時的にIP電話サービスのご利用を停止する場合に利用します。 (1) 停止方法 ①ハンドセット（受話器）を取りあげ「＊＊＊04」をダイヤルしてください。 ②ダイヤルが終了すると「ププ」という音が聞こえますのでハンドセット（受話器）を置いてください。それで登録が終了です。 (2) 開始方法 ①ハンドセット（受話器）を取りあげ「＊＊＊05」をダイヤルしてください。 ②ダイヤルが終了すると「ププ」という音が聞こえますのでハンドセット（受話器）を置いてください。それで登録が終了です。 ※プッシュホン信号を送出できる電話機をご使用ください。（信号種別を変更できる電話機をご使用の場合は、「PB」に切り替えればご使用になれます。）	サービス指定 （[IP電話サービス] IP電話サービス）

ルータ機能

サービス機能	内　容	Web画面
PPPoE接続 （マルチセッション対応）	プロバイダのPPPoEサーバと認証を行い、ネットワーク情報（IPアドレスなど）を取得してLAN側のパソコンがインターネットへ接続できるようにする機能です。マルチセッションに対応し、2つ以上の接続先と同時に通信することができます。 ※ご利用のネットワークのセッション数以上の設定を有効にした場合は、フレッツ・セーフティの機能がご利用できなくなります。 ※1つのセッション（「接続先5」）はフレッツ・スクウェア固定となります。	ネットワーク設定 （動作モード） PPPoE設定
DHCPクライアント	DHCPサーバよりIPアドレスなどを取得することでネットワーク情報（IPアドレスなど）を取得してLAN側のパソコンがインターネットへ接続できるようにする機能です。	ネットワーク設定 （動作モード）

サービス機能	内　容	Web画面
固定IP	WAN側ネットワーク設定（IPアドレスなど）を、本商品に固定的に設定することで、LAN側のパソコンがインターネットへ接続できるようにする機能です。（ただし、フレッツ・ADSL、Bフレッツを接続を利用してプロバイダから固定IPアドレスを割り当てられる場合には、動作モードを「PPPoE」にします。）	ネットワーク設定（動作モード）
DNSリレー	LAN側のパソコンからのDNS問い合わせに対し、本商品がWAN側のDNSサーバに代理で問い合わせて名前解決を行います。DNSプロキシとも言います。DNSへの問い合わせを接続先1～5で振り分けることができます。	DHCP設定（DNS サーバアドレス） ルーティング条件（サブセッション）
NTP機能	インターネット上に存在するNTPサーバのアドレスを本商品に設定することにより、本商品の内部時計をNTPサーバが提供する正確な時刻に合わせることができます。	ネットワーク設定（NTPサーバIPアドレス）
Unnumbered接続	プロバイダから割り当てられた複数の固定IPアドレスを本商品やパソコンに設定してグローバルIPアドレスによるネットワークを構築することができます。インターネットサーバ公開などが可能です。 ※Unnumbered接続時には、ハッカーの不正アクセスをブロックする機能の一部が効かなくなります。	PPPoE設定(IPアドレス指定)
DHCPサーバ機能	LAN側のパソコンが起動すると、その都度IPアドレスなどのネットワーク利用に必要な設定情報を本商品から各パソコンへ自動的に割り当てます。各パソコンでネットワークの詳細な設定を行わなくてもLANやインターネットへ接続することができます。	DHCPサーバ設定
IPマスカレード機能（NAPT）	1つのグローバルアドレスを利用してLAN側のプライベートアドレスをもつ複数のパソコンをインターネットに接続することができます。LAN側のパソコンのIPアドレスが外部に流出することを防ぐことができます。	NAPT設定
UPnP機能	UPnP機能対応アプリケーションをNAPT機能の実装に関係なく、複雑な設定をせずに簡単に利用することができます。 マルチセッション使用時は設定により接続先1～5のいずれかのみ制御可能となります。 ※UPnP機能を有効に設定すると、セキュリティ機能の一部がご利用できない場合があります。 ※Windows® XP以外のOSでUPnP機能をご利用になる場合は、お使いのパソコンにUPnPドライバがインストールされていることをご確認ください。	NAPT設定（UPnP設定）

（次ページに続く）

機能仕様

サービス機能	内　容	Web画面
簡易DMZ	グローバル側からのアクセスをLAN側の特定の端末へすべて転送します。NAPTを使用すると通信が行えないネットワークゲームなどに使用するときに用います。 バーチャルコンピュータ（Virtual Computer）とも称します。	NAPT設定 (簡易DMZ IPアドレス)
サーバホスティング機能	グローバル側の指定ポートへのアクセスを指定端末の指定ポートへ転送します。LAN側のサーバをインターネットに公開する場合に用います。	NAPT設定 (静的NAPT設定)
IPアドレス/ポートフィルタ機能	WAN側およびLAN側からのアクセスをIPアドレス/ポート番号を指定することで外部からの不正なアクセスを規制したり、内部からの情報漏洩を防ぎます。 接続先1～5からのアクセス規制も可能です。 ※ウイルス検索の対象が使用するポート（25（メール送受信：SMTP)、80（Web：HTTP)、110（メール受信：POP3)）についてはIPアドレス／ポートフィルタ機能はご利用できません。	IPフィルタ設定
ルーティング（静的）	パケットを宛先に届けるための経路を選択する機能です。経路情報を固定的に設定します。 接続先1～5への設定が可能です。	ルーティングテーブル設定 ルーティング条件（メインセッション） ルーティング条件（サブセッション）
VPN（バーチャルプライベートネットワーク）機能	LAN側に接続したパソコンをプライベートネットワーク（VPN）に収容することができます。 サポートしている暗号化方式プロトコルは、PPTP、IPSec、L2TPの3種類です。 パソコンにVPN対応ソフトウェアをインストールする必要があります。 ※VPNをご使用する端末に対しては、セキュリティ機能の一部がご利用できない場合があります。	VPNパススルー設定
SPI（ステートフルパケットインスペクション）機能	IPアドレス、ポートフィルタを通過するパケットのデータを読み取り、内容を判断して動的にポートを開放・閉鎖する機能です。 本商品のIPアドレス/ポートフィルタ機能と併用することで、セキュリティ機能をより強めることができます。	SPI（ステートフルパケットインスペクション）設定
Dynamic DNS機能	Dynamic DNSサービスを利用することができます。 WAN側IPアドレスが変わっても、LAN側のパソコンにつけたホスト名で外部からアクセスすることができます。	Dynamic DNS設定
ルーティング（動的）	パケットを宛先に届けるための経路を選択する機能です。自動的に経路情報を設定します。 RIP version1に対応します。 接続先1～4の指定が可能です。	RIP設定

サービス機能	内　容	Web画面
Windows共有フィルタ	Windowsネットワークで共有機能を実現するプロトコル（NetBIOS等）によるWAN側との通信を遮断し、LAN内の共有ファイル/プリンタの不正使用や、内部情報の流出を防止します。	Windows共有フィルタ/ステルス設定（Windows共有フィルタ）
ステルス機能	WAN側からの不正アクセスを防止します。 本商品はTCPパケット/UDPパケット/ICMPパケットのそれぞれのアクセスを防止する/しないを選択することができます。 TCPステルスモード 　TCPプロトコル上で使用可能となっていないポートに対して送られたパケットに応答しません。 UDPステルスモード 　UDPプロトコル上で使用可能となっていないポートに対して送られたパケットに応答しません。 ICMPステルスモード 　ICMPパケット（障害発生時やネットワーク管理のために使用するパケット）に応答しません。	Windows共有フィルタ/ステルス設定（ステルスモード設定）
IPv6ブリッジ	PPPoEの場合に、本商品のLAN側に設置されたパソコンとIPv6ネットワークでインターネット接続を利用することができます。 IPv6プロトコルを利用したパケットについて、WAN-LAN間で全てブリッジします。 PPPoE接続先1～5が接続中でも使用できます。 IPv6サービスを利用するときに使用します。 ※IPv6の通信については、本商品のセキュリティ機能はご利用いただけませんのでご注意ください。	ネットワーク設定（IPv6ブリッジ設定）

機能仕様

無線機能

サービス機能	内　容	Web画面
無線LAN	無線LANカード（Web caster FT-STC-Oa/gもしくはWeb caster FT-STC-Va/g）を本商品に装着することにより、IEEE802.11b、IEEE802.11g、IEEE802.11a準拠の無線LANのアクセスポイントとして動作します。 無線LANカードを装着したパソコンと無線LAN通信を行うことができます。	無線LAN設定 （基本設定）
無線LANカードを装着したパソコンからのアクセス制限	無線LANカードを装着したパソコンからの通信を制限することができます。パソコンのMACアドレスを本商品に設定する必要があります。	無線LAN設定 （MACアドレスフィルタリング）
ANY接続	クライアント側で接続先のアクセスポイント（本商品）のESSIDに「ANY」もしくは「空白」を設定しておけば、アクセスポイントがどんなESSIDを設定していても接続できてしまう機能です。アクセスポイント側でANY接続を「許可/拒否」の選択が可能です。「拒否」を設定している場合は、ANY接続はできません。	無線LAN設定 （基本設定）
暗号化	無線LANネットワーク内のデータを他人に見られたり、不正に利用されないための通信データの暗号化する機能があります。暗号化方式としては以下のものをサポートしています。 ①WEP 一般的な暗号化方式。キー入力方法には直接入力方法とPass Phrase（WEPキー生成アルゴリズム）によるキー生成方法があります。 ②TKIP WEPの脆弱性を補い、セキュリティの強化、ユーザー認証機能の装備やキーの定期的な更新などを考慮したWPA（ Wi-Fi Protected Access ）という暗号化の規格があります。 WPAの認証方法の「事前共有キー（WPA-PSK（Pre-Shared key））」で使用する暗号化方式の1つです。	無線LAN設定 （暗号化設定）

セキュリティ機能

サービス機能	内　容	Web画面
セキュリティ （フレッツ・セーフティ対応機能）	Bフレッツかフレッツ・ADSLをご利用いただいているお客さまに提供するセキュリティサービスです。 本商品のセキュリティ対策ファイルを、フレッツ網に設置したフレッツ・セーフティ専用装置により常に最新のバージョンにバージョンアップすることで、e-mailのウイルス検知・駆除機能ならびに不正アクセス防止機能を提供いたします。 ご利用には、申し込み時の初期費用と月額料金が別途必要となります。	かんたん設定 セキュリティ（ウイルス対策設定）

その他

サービス機能	内　容	Web画面
オート・ネゴシエーション（自動切替え）	WAN側／LAN側は以下のインタフェースを利用することが可能です。（接続すると自動的に識別するため本商品のデータ変更は必要ありません。）固定設定も可能です。 LAN側は各ポート毎に設定が可能です。 以下の動作モードおよび通信速度切替を行います。 ・100Mbps 全二重通信 ・100Mbps 半二重通信 ・10Mbps　全二重通信 ・10Mbps　半二重通信	ネットワーク設定 （[ポート設定] WAN ポート設定 /LAN1～4 ポート設定）
パソコンの複数接続	LAN側が4ポート収容可能であり複数台のパソコンを接続することができます。また、無線機能をご使用することでも複数台のパソコンを本商品に接続することができます。	ネットワーク設定 他
停電中の扱い	停電中はIP電話サービスをご利用できません。（加入電話回線のご利用となります。）	
Webブラウザによる設定	Webブラウザをご利用いただくことで本商品の各種条件の変更や状態を確認することができます。 「2 詳細設定方法」（☛P2-1）	ネットワーク設定 （LAN側IPアドレス /マスク長） パスワード設定 （Web設定ログイン パスワード設定）
バージョンアップ （自動バージョンアップ機能を利用してバージョンアップする）	本商品がインターネット上の当社のサーバに登録された最新のファームウェアやセキュリティ対策ファイルを確認したときに、自動で本商品のプログラムを最新版に更新することができます。（取扱説明書「自動バージョンアップ機能を利用してバージョンアップする」）	アップデート設定 自動アップデート （実行時刻）
バージョンアップ （バージョンアップお知らせ機能を利用してバージョンアップする）	バージョンアップお知らせ用サーバに最新版のプログラムが登録されたことを本商品がサーバへ自動的にアクセスし確認することができます。登録が確認できた場合はプログラムを最新版に更新してください。 電話機からの操作またはWebブラウザをご利用いただくことで実施可能です。 （1）電話機からの操作 ①ハンドセット（受話器）を取りあげます。 「ピーピーピー…」という音が約2秒間聞こえ、その後通常の発信音「ツー」に切り替わります。 ②「＊＊＊11」をダイヤルします。ダイヤルが終了すると「ププ」という音が聞こえます。	状態表示1 （ファームウェア 手動アップデート）

（次ページに続く）

機能仕様

<table>
<tr><th>サービス機能</th><th>内　容</th><th>Web画面</th></tr>
<tr>
<td>バージョンアップ（バージョンアップお知らせ機能を利用してバージョンアップする）</td>
<td>
③ハンドセット（受話器）を置いてください。（バージョンアップを開始します。）
バージョンアップ実行中、本商品のランプ表示は以下のようになります。
<table>
<tr><th>ランプの種類</th><th>ランプのつき方</th></tr>
<tr><td>ALARMランプ</td><td>遅い点滅（赤）</td></tr>
<tr><td>PPPランプ</td><td>遅い点滅（緑）</td></tr>
<tr><td>VoIPランプ</td><td>遅い点滅（緑）</td></tr>
<tr><td>TELランプ</td><td>遅い点滅（橙）</td></tr>
</table>
※バージョンアップ中に電源を切らないでください。回復不能な故障の原因になることがあります。
※バージョンアップ実行中（数分間）はインターネット接続が切断されます。バージョンアップ実行中にダウンロードなどを実行している場合はご注意ください。
④本商品のランプ表示が以下のようになればバージョンアップは終了です。
<table>
<tr><th>ランプの種類</th><th>ランプのつき方</th></tr>
<tr><td>POWERランプ</td><td>点灯（緑）</td></tr>
<tr><td>ALARMランプ</td><td>消灯</td></tr>
<tr><td>PPPランプ</td><td>点灯（緑）：
1セッション接続時
点灯（橙）：
2セッション以上接続時</td></tr>
<tr><td>VoIPランプ</td><td>点灯（緑）</td></tr>
<tr><td>TELランプ</td><td>点灯（橙）</td></tr>
<tr><td>WANランプ</td><td>点灯（緑）または点滅（緑）</td></tr>
<tr><td>HACKERランプ</td><td>点灯（緑）</td></tr>
<tr><td>VIRUSランプ</td><td>点灯（緑）</td></tr>
</table>
※プッシュホン信号を送出できる電話機をご使用ください。（信号種別を変更できる電話機をご使用の場合は、「PB」に切り替えればご使用になれます。）
（2）Webブラウザからの操作（取扱説明書「バージョンアップお知らせ機能を利用してバージョンアップする」）
</td>
<td>状態表示1
（ファームウェア手動アップデート）</td>
</tr>
</table>

サービス機能	内　容	Web画面
バージョンアップ（当社ホームページからプログラムをダウンロードしてバージョンアップする）	Webブラウザをご利用いただくことで本商品のプログラムを最新版に更新することができます。 ホームページからパソコンへいったんプログラムをダウンロードしたあとパソコンから本商品への反映を実施してください。（取扱説明書「当社ホームページからプログラムをダウンロードしてバージョンアップする」）	ファームウェア更新
特番一覧	本商品で利用可能な特番は以下になります。 ＊＊＊02：直前の通話相手の着信を次回以降拒否します。(「着信拒否」(☛P5-3)) ＊＊＊03：着信拒否リストの登録情報を、全て抹消します。(「着信拒否」(☛P5-3)) ＊＊＊04：IP電話機能を無効にします。(「IP電話サービス利用停止」(☛P5-4)) ＊＊＊05：IP電話機能を有効にします。(「IP電話サービス利用停止」(☛P5-4)) ＊＊＊11：本商品のバージョンアップを行います。(「バージョンアップ（バージョンアップお知らせ機能を利用してバージョンアップする)」(☛P5-9)) ダイヤルの最後に"#"： ダイヤル入力の終了 ※プッシュホン信号を送出できる電話機をご使用ください。（信号種別を変更できる電話機をご使用の場合は、「PB」に切り替えればご使用になれます。）	

用語集

【アルファベット順】

ADSL	(Asymmetric Digital Subscriber Line) 非対称型ディジタル加入者回線。従来の電話線（加入電話回線）を用い、電話の音声を伝えるのには使わない高い周波数帯を使ってデータ通信を行います。ユーザ方向へのデータ通信を「下り」、逆方向を「上り」と言い、ADSLでは、下りの通信速度が、上りの通信速度よりも大きくなるように通信帯域の割り当てを行っています。
ADSLモデム	(ADSL Modem) ADSL回線と接続して、Ethernet LAN信号と加入電話回線を通じて送受信するADSL信号の相互変換を行う装置です。ADSLモデムとコンピュータの間はEthernet LANでつなぎます。
ANY接続	無線LANクライアントの設定で、接続先アクセスポイントのESSIDを空欄または「ANY」に設定した場合に、ESSIDが一致しなくてもアクセスポイントに接続が可能になる方法のことです。本商品はANY接続を許容する機能がありますが、セキュリティ上の問題から、ANY接続を許容しないアクセスポイントもあります。
CHAP	(Challenge Handshake Authentication Protocol) PPPで接続のときにユーザを認証するために利用する認証用プロトコルです。PAPと異なり、暗号化された認証情報をネットワーク上でやり取りするため、安全性が高いという特長があります。
DHCP	(Dynamic Host Configuration Protocol) ネットワーク上のDHCPサーバから、IPアドレスやサブネットマスクなどの設定情報を取得することで、自動的にネットワーク接続を可能にする方式です。動作モードがDHCPのとき本商品のWAN側ポートはDHCPクライアントとなります。LAN側ポートに接続されたコンピュータに対しては本商品はDHCPサーバとなります。
DHCP クライアント	(DHCP Client) ネットワーク上のDHCPサーバから接続に必要なIPアドレス等を割り当ててもらうシステムです。
DHCPサーバ	(DHCP Server) ネットワーク内の接続設定情報を管理し、DHCPクライアントからの要求に応じて、接続に必要なIPアドレス等を割り当てるシステムです。
DNS	(Domain Name System) インターネットにおいて、ホスト名を表わす名前（文字列）から、それに対応するIPアドレスを検索するシステムです。また、その逆の検索も行います。 本商品のLAN側IPアドレスには「setup.fletsphone」という名前が対応しています。

DNSサーバ	(Domain Name System Server) ホスト名とIPアドレスとの対応表を持っており、ホスト名の問い合わせにIPアドレスを通知したり、逆に、IPアドレスの問い合わせにホスト名を通知するサーバです。
DNSリレー	(Domain Name System Relay) LAN側のパソコンなどから、PPPやDHCP等で取得したDNSサーバアドレスに対して、DNS問い合わせがある場合に、その問い合わせを中継して名前解決を行う機能です。
DSP	(Digital Signal Processor) ディジタル信号処理専用のマイクロプロセッサです。音声や画像などの処理に特化しています。
Dynamic DNS	(Dynamic Domain Name System) IPアドレスを指定せずにドメイン名で指定できるようにする機能です。ホスト名とIPアドレスとの対応に変更があった場合（例：プロバイダから本商品に異なるIPアドレスを割り振られた場合など）新しいIPアドレスを取得するごとにIPアドレスをDNSサーバに通知して、IPアドレスが変わっても同一のドメイン名を継続して利用できるようになります。サーバを公開する場合に有効です。
ESSID	(Extended Service Set Identifier) 無線LANで、ネットワークを識別するための情報です。本商品にESSIDを設定しておき、接続するパソコン等にも同じESSIDを設定しておけば、通信が可能になります。接続するネットワークをESSIDで指定することができます。ESSIDはセキュリティ機能の一つに分類される場合もありますが、あくまでも接続先の識別機能ですので、ESSIDを設定後に他のセキュリティ設定をすることをお勧めします。
FTP	(File Transfer Protocol) ネットワーク上のクライアントとホストコンピュータとの間で、ファイルの転送を行うためのプロトコルです。
FQDN	(Fully Qualified Domain Name) ホストやドメインを指定する場合にドメイン名部分の文字列を省略せずにすべて記述する表記方法です。
HTML	(HyperText Markup Language) Webページを記述するためのマークアップ言語です。タグを付ける（マークアップする）ことによって、文書の構造や見栄えを指定したり、文書の中に画像や音声等へ移動するためのハイパーリンクを埋め込むことができます。
HTTP	(HyperText Transfer Protocol) インターネット上でHTMLファイルをWebブラウザがWWWサーバに対して送受信するときに利用するプロトコルです。リクエストとレスポンスからなるプロトコルで、それぞれリクエストとレスポンスが独立した通信の単位になります。TCP上で動作します。

用語集

用語	説明
ICMP	(Internet Control Message Protocol) TCP/IPプロトコルにおいて、その機能を補助するために用意された制御用のプロトコルです。TCP/IPパケットの転送中において発生した各種のエラーの通知や、動作の確認などを行うために利用されます。
IEEE802.11/802.11a/802.11b/802.11g	無線LAN通信に関する国際規格IEEE802.11を拡張したもので、IEEE802.11aはIEEEが標準化した5GHz帯の電波を使い最大54Mbpsの転送速度の無線LANの物理層の規格、IEEE802.11bはIEEEが標準化した2.4GHz帯の電波を使い最大11Mbpsの転送速度の無線LANの物理層の規格、IEEE802.11gはIEEEが標準化した2.4GHz帯の電波を使い最大54Mbpsの転送速度の無線LANの物理層の規格です。本商品を屋内で使用する場合は11aをお試しになり、通信に支障があれば11b/gで通信を行ってください。また、電波法により屋外での11aの使用は禁止されています。
IP	(Internet Protocol) 異なるネットワークの間でパケットの転送を行うための取り決めを表します。IPアドレスにより相手先を判断します。IPv4 (Internet Protocol Version 4) とIPv6 (Internet Protocol Version 6) の2つがあります。
IPSec	(Security Architecture for the Internet Protocol) IPのパケットを暗号化し、インターネット上で通信するための規格。VPNで最も広く使用されています。
IPv6	(Internet Protocol Version 6) 現在広く使われているIP (IPv4) の発展型として開発された新しいIPです。IPアドレスの長さが32ビットのIPv4では、世界で約40億台のコンピュータが接続できますが、1990年代に入ってからはインターネットの普及により接続台数が急増したため、IPv6ではIPアドレスの長さが128ビットに拡張されています。パケットヘッダの簡素化、セキュリティ機能の追加などが盛り込まれて、IPv4にあったさまざまな問題点が解消されています。
IPアドレス	(Internet Protocol Address) ネットワーク上で機器を特定するためのアドレスです。例えば、IPv4では192.168.1.1のようにピリオドを挟んだ4つの数字 (0～255) で表します。
IP電話	インターネットなどのIPネットワーク上で音声データを転送する技術です。音声データとIPデータの変換を行います。
IPパケットフィルタリング	(Internet Protocol Packet Filtering) ネットワークを流れるデータ (IPパケット) を選別し、そのデータを通過させるか (許可)、させないか (拒否) を指定することで、外部から流れてくる不要なデータを遮断したり、逆に内部からデータ漏洩を防ぐ技術です。

LAN
（Local Area Network）
会社内や家庭内など、比較的に狭い空間でコンピュータや周辺機器を接続したネットワークシステムです。ファイルやプリンタなどを共有することが可能となります。

L2TP
（Layer 2 Tunneling Protocol）
インターネット上に生成した仮想的なトンネルを通じてPPP接続を確立し、VPNを構築するプロトコルです。類似のプロトコルにIPsecなどがありますが、L2TPはハードウェアに依存した情報を利用することでアクセスの制御を実現できるという特長があります。

MACアドレス
（MAC Address）
すべてのネットワーク機器は固有の番号としてMACアドレスという6バイト（12桁）の番号を持っています。MACアドレスはLANに接続されている機器を識別するためのアドレスです。

MACアドレスフィルタリング
（MAC Address Filtering）
無線LAN端末固有のMACアドレスを無線LANアクセスポイントに設定する事で、無線LAN端末を無線LANアクセスポイントに接続するか否かを制御するセキュリティ方式です。

MTU
（Maximum Transmission Unit）
ネットワークにおいて、1回で送信できる1パケットのデータの最大値を示します。MTUの単位はバイトです。PPPoEでは通常1454といわれていますが、Webサイトにより1454ではアクセスできず、4の倍数で1454より小さい値を推奨しているものがあり安全のために本商品では1452としています。

NAPT
（Network Address Port Translation）
LANで利用されるプライベートIPアドレスをグローバルIPアドレスに変換する仕組みです。これにより、複数の機器が1つのグローバルアドレスを利用して接続ができるようになります。

NetBIOS
（Network Basic Input/Output System）
ネットワーク環境を実現するトランスポート層やセッション層のネットワーク・サービスを呼び出すためのAPIインターフェイスです。下位プロトコルに、TCP/IP（ポート137、138、139:Windows® 2000/XPでは、さらにポート445）が使われます。
主としてLAN（ローカル・エリア・ネットワーク）環境やイントラネット環境を想定したものであり、WAN接続やプロバイダ接続する場合などは離れた場所でも、ファイル共有、プリンタ共有が使えるなどの利点はありますが、「不必要な情報」が外部へ流出する可能性があります。本商品はNetBIOSによる情報の外部流出を防止することができます。また、ロケーション・サービス（TCP/UDPポート番号135）に対しても同様の処置がとられます。

用語集

NTP	(Network Time Protocol) ネットワークを介して時刻を調整するプロトコルです。具体的には、クライアントの内部時計の時刻を、インターネット上に存在するNTPサーバを介して調整します。
PAP	(Password Authentication Protocol) ユーザIDとパスワードを使用する認証用プロトコルです。PPPの接続を確立するときなどに利用されます。
PING	ICMPの機能を利用したコマンドで、TCP/IPネットワークにおいてパケット通信テストを行います。ネットワーク機器が接続されているかどうかの確認に利用します。
PPP	(Point-to-Point Protocol) 電話回線を通してインターネット接続するときに利用されることの多い接続方式です。認証機能などがあります。
PPPoE	(Point-to-Point Protocol over Ethernet) Ethernetなどのネットワーク上で、PPPのような利用者の認証を行なうための方式です。フレッツ・ADSLやBフレッツではPPPoEを利用することで、指定されたプロバイダに接続するためのユーザ名、パスワードのチェックを行い、また利用者へのIPアドレスの割り当ても可能にしています。PPPoEには接続先を選択するサービスもあり、利用者は入力するユーザ名とパスワードを変更することで接続先プロバイダを変更することもできます。PPPoEを利用するには、PPPoEのクライアント機能を持つソフトウェアが必要です。本商品はPPPoEクライアント機能を備えているため、パソコンなどにソフトウェアをインストールしなくてもPPPoEを利用することができます。
PPTP	(Point to Point Tunneling Protocol) 米インターネット上で暗号化された情報を送受信する時に使用されるプロトコルで、VPNを実現するために利用されています。PPPというプロトコルを拡張したものです。
RIP	(Routing Information Protocol) TCP/IPなどによって構成されるネットワークにおいて、動的なルーティング制御を行うためのプロトコルです。ルータなどの制御機器どうしが経路情報を交換し、それによって得た経路情報(ルーティングテーブル)を元に、現在地から宛先までの最適なルートを判定します。
SLIC	(Subscriber Line Interface Circuit) 電気通信事業者の設備と加入者の間を結ぶ回線のことです。
SIP	(Session Initiation Protocol) インターネットを通じて指定した相手と通信を制御するためプロトコルで、主にIP電話などで用いられています。

SIPサーバ
（SIP Server）
IP電話サービスネットワーク内に設置され、各装置のIP電話サービスへの登録および、装置間の通話確立などを仲介するサーバです。プロキシサーバ、レジスタサーバから構成します。

SPI
（Stateful Packet Inspection ）
ファイアウォールを通過するパケットの内容を読み取り、ポートの開放と閉鎖を行います。
LAN側の端末から送信されたパケットのセッション情報をログに記録しておき、WAN側から到着したパケットが、このログにあるセッション情報に応じたものであることを確認したときは、このパケットをLAN側へ流します。

TCP
（Transmission Control Protocol）
データの転送を制御するプロトコルです。送信先に接続してデータ送信をします。受信側は受け取ったパケットの到達確認を行い、エラーを訂正する機能を持つので、信頼性の高い通信を実現できます。TCP/IPプロトコル群の中では、IPとともに主要な伝送制御プロトコルになります。

TCP/IP
（Transmission Control Protocol/Internet Protocol）
インターネットでの標準プロトコルです。TCP/UDPとIPというそれぞれのプロトコルを用いて通信を行います。

TKIP
（Temporal Key Integrity Protocol）
従来の暗号化であるWEPの脆弱性を克服するために、キーを自動的に変更して暗号化を行うように改良された暗号化方式の1つです。
定期的に使用する暗号化キーを変更するために、キーの解析が困難となり、WEPより強固なセキュリティとなります。

UDP
（User Datagram Protocol）
データの転送を制御するプロトコルです。TCPとは異なり受信側へ接続をせずに送信します。このため、高速に通信することが可能です。

Unnumbered
（Unnumbered）
他のネットワークに接続するルータのWAN側ポートにIPアドレスを割り当てず、2台のルータを見かけ上1台のルータのように扱う接続方式です。Unnumberedで運用されているルータは、IPアドレス変換機能を無効にして固定IPアドレス（グローバルIPアドレス）をLAN側のパソコンに割り当てます。
Unnumbered接続を行う場合、2台のルータが繋がっているネットワークに他のコンピュータがいるとパケットの行き先が確定しなくなるため、ルータどうしが直結している必要があります。

UPnP
（Universal Plug and Play）
特別な設定なしに機器をLANに接続し通信することができます。ネットワーク間にルータを接続しNAPT機能などを実装していてもLAN内の機器が外部と通信可能です。

用語集

用語	説明
URL	(Uniform Resource Locator) インターネット上の情報資源（文書や画像など）の場所を指し示す記述方式です。インターネット上に存在する情報のアドレスと、アクセス方法を特定します。
VDSL	(Very high-bit-rate Digital Subscriber Line) 超高速非対称型ディジタル加入者回線。通常の電話回線を利用して高速通信を実現するものです。ADSLよりも高速ですが伝送距離が短いため、建物内部の通信などに使用します。
VDSLモデム	(VDSL Modem) コンピュータをVDSL回線に接続するときに必要になる、信号を相互に変換する装置です。
VPN	(Virtual Private Network) 企業などでプライベートネットワーク専用の回線を設置する場合、工事や維持管理に膨大な費用を投入しなければなりませんが、情報を暗号化して電話回線やインターネット上で通信するシステムを構築すれば、費用を安く抑えることができます。VPNはこれを実現するためのネットワークシステムです。
VPNクライアント	VPNに接続している端末を指します。
WAN	(Wide Area Network) 広域のネットワークを意味します。LANと対比して利用されることがあり、伝送距離に制限がないことが特徴です。
Webブラウザ	(Web Browser) Webページ(WWWシステムを使ってインターネット上で公開されている文書)を閲覧（ブラウザ）するためのソフトウェアです。代表的なものとしてInternet Explorerがあります。
WEP	(Wired Equivalent Privacy) IEEE802.11という無線LANの規格に含まれる、標準の暗号化方式です。無線通信は傍受が極めて容易であるため、送信されるパケットを暗号化して傍受者に内容を知られないようにすることで、有線通信と同様の安全性を持たせようとしています。
WEPキー	WEPで用いられる秘密の鍵です。送信者と受信者は同じ鍵を登録した上で通信を行います。
WEPキー pass phrase	(パスフレーズ) パスワードの長くなったものをWEPキーでは使用しています。複数の単語を羅列することにより、より高度なセキュリティ性を実現しています。

WPA-PSK情報	WPA-PSK（Wi-Fi Protected Access Pre-shared key）はWEPに脆弱な点を補強しセキュリティ性を向上させたプロトコルです。ユーザの認証や秘密鍵の定期的な自動更新を実現しています。PSKはWPAにおいて事前共有鍵を設定する方式です。WPA-PSK情報というのは、この両者を組み合わせた認証方式の情報を指します。

5
付録

用語集

【あいうえお順】
【あ行】

アカウント
(Account)
ネットワークに接続(ログイン)するときの権利を意味します。具体的にはログインIDを指し、プロバイダと契約した際に通知されるIDのことです。プロバイダによっては、ログインIDの呼び方が異なります。

アクセスポイント
「インフラストラクチャ・モード」での通信の中継点となるポイントです。有線LAN接続のパソコンでは、アクセスポイントと通信することで無線LAN接続のパソコンと通信します。

イーサネット
(Ethernet)
現在、最も普及しているLANです。10BASE-Tや100BASE-TXなどの規格があります。

インフラストラクチャ・モード
(infrastructure mode)
無線LANの通信方式の一つで、無線LANクライアントがアクセスポイントを介して通信を行なうモードのことです。アクセスポイントを介さずに通信を行なう場合は、「アドホック・モード」などと呼びます。

ウイルス検索エンジン
(virus search engine)
コンピュータウイルスを除去するためのソフトウェアです。ウイルス検索エンジンやウイルスパターンが常に最新ものでない場合、このソフトウェアが正常に動作しないことがあります。

ウイルスパターン
(virus pattern)
ウイルスパターンとは、コンピュータウイルスの1つ1つが固有に持っている独自コードのことです。ウイルスを解析してウイルスパターンを抽出することによりウイルスを識別することが可能となります。ウイルス検索エンジンは、パターンファイルを参照しながら検査対象となるファイルの中に登録されているウイルスパターンがないかどうかを調べます。

オンライン登録
(Online Registration)
フレッツ・セーフティ対応のサービスをご利用になる際に、ユーザ登録をWebブラウザで実施する登録サービスです。(☛P2-6)

【か行】

回線終端装置	(Digital Service Unit) ディジタル回線に端末装置を接続するための終端装置です。Bフレッツでは ONU（Optical Network Unit）などを指します。
簡易DMZ	(Simplicity De-Militarized Zone) WAN側からのアクセスをLAN側の特定の端末へすべて転送します。NAPTを使用すると通信が行えないネットワークゲームなどに使用するときに用います。バーチャルコンピュータ（Virtual Computer）とも呼ばれます。
グローバルIP アドレス	(Global IP Address) インターネットへ接続している端末に一意に割り当てられるIPアドレスです。インターネット上での住所のようなもので、他に重複するもののない、世界で唯一のIPアドレスのことです。日本ではJPNIC（社団法人 日本ネットワークインフォメーションセンター）という機関がグローバルIPアドレスを管理しています。
ゲートウェイ	(Gateway) プロトコルの異なるLANどうしやLANとWANとを接続する装置です。

【さ行】

サブネットマスク	(Subnet Mask) コンピュータどうしが同じネットワーク部であるかを判断するための値です。例えば、255.255.255.0のようにピリオドを挟んだ4つの数字（0～255）で表します。
ステルスモード	(Stealth Mode) WAN側からの不正アクセスを防止します。 本商品はTCPパケット/UDPパケット/ICMPパケットのそれぞれのアクセスを防止する/しないを選択することができます。
スループット	(Throughput) コンピュータが処理を行う速度を意味します。CPU、メモリ、ハードウェア等がそれぞれ影響しあった結果、すべての要素を通して、最終的に処理がどれほどの速度で行われるかを指します。
セキュリティ対策ファイル	本商品のセキュリティ機能において使用するウイルス検索エンジン、ウイルスパターン、ファイアウォールルールの総称です。
セッション	(Session) ネットワークまたはリモートコンピュータに接続している状態を意味します。例えば、ログインのことを「セッションの開始」といい、ログアウトのことを「セッションの終了」ともいい、接続してから切断するまでの状態になります。

用語集

【た行】

チャネル

（channel）
無線通信では、使用する周波数帯域を分割して、それぞれの帯域で異なる通信を行うことができます。チャネルとは、その分割された個々の周波数帯域のことです。複数の無線LANを狭いエリアで同時使用する場合は、それぞれに異なる周波数を割り当てないと、無線干渉が発生して、通信速度が遅くなる場合があります。その場合、なるべく各チャネル同士の帯域が重ならないような使用を推奨します。

【な行】

ドメイン

（domain）
「領地」を意味し、ネットワーク関連では、ある組織やサイトなどがひとまとまりとなっている管理単位を表します。

ネットワークアドレス

（Network Address）
IPアドレスの中のネットワークを識別する部分です。IPアドレスはネットワークアドレス部とホストアドレス部に分かれ、ネットワーク全体の中でサブネットを識別するために使われる部分がネットワークアドレス部になります。例えばサブネットマスクが255.255.255.0の場合は、IPアドレスの3つ目のピリオドまでの数字がネットワークアドレスになります。

【は行】

パケット

（packet）
一定のサイズに分割されたデータの先頭に、データの属性や宛先などを付けたものです。

パケット通信

（packet communication）
パケット化されたデータを送受信する通信のことです。携帯電話やISDN等で利用されています。

パススルー

信号を何の処理もしないで通過させることです。

パスワード

（Password）
コンピュータ・システムの安全性や信頼性を維持するために利用される、数字や文字列による符号です。パスワードを設定する際は、名詞や単純な数字、文字は避け、文字、数字、記号を組み合わせて設定することや、定期的にパスワードを変更することが望まれます。

パターンファイル

（pattern file）
ウイルスパターンを登録しているデータベース・ファイルのことです。

ハッカー	元来はコンピュータ分野において優れた技術を発揮する人のことを指していましたが、他人のコンピュータに不正なやり方で侵入し、破壊活動などを行う人をも指すようにもなった名称です。
ファームウェア	(firmware) ハードウェアの基本的な処理を行うため、コンピュータ機器などに組み込まれたソフトウェアのことです。
ファイアウォール	(fire wall) 外部からの不正なアクセスを防ぐためのシステム。LANとインターネットの間で不正なアクセスの検出や遮断を実現しています。
ファイアウォールルール	(fire Wall rule) ファイアウォールが特定パケットの通過を許可もしくは拒否するための設定です。
プライベートIPアドレス	(Private IP Address) 外部のネットワークに直接接続することのない端末に対し、企業や組織内で自由に設定できるIPアドレスです。インターネット通信は、ProxyサーバやNAT(Network Address Translator)などを使って実現しています。
プロキシサーバ	(Proxy Server) SIPを使った各装置からSIPプロトコルメッセージを受け取り、相手先に代理送信することにより装置間の通話を確立させるサーバです。
プロトコル	(Protocol) データ通信を行うための必要な取り決めを意味します。TCPやUDP、IPなど、数多くの種類があります。
プロバイダ	(Internet Services Provider) インターネットの接続サービスを提供している事業者を表します。
フレッツ・セーフティ	フレッツ・セーフティはフレッツ・ADSLまたはBフレッツご利用のお客さまに対し、NTT東日本またはNTT西日本のフレッツ網上に設置したフレッツ・セーフティ専用装置よりお客さま宅に設置されたフレッツ・セーフティ対応機器のメールのウイルス検知・駆除機能、不正アクセス防止機能の維持・管理をオンラインで行うサービスです。本商品の設定画面からオンライン登録を実施していただくことでご利用いただけます。フレッツ・セーフティのご利用には、申込時の初期費用と月額料金が別途必要となります。
フレッツ・スクウェア	フレッツ・スクウェアは、NTT東日本もしくはNTT西日本のフレッツ網に開設しているフレッツ・シリーズご利用者専用サイトです。お客さま宅までの回線速度測定など、さまざまなコンテンツが用意されています。

用語集

ポート	(Port) インターネット通信において複数の相手と同時に接続を行なうために、IPアドレスの下に設定されているサブ(補助)アドレスです。TCP/IPで通信を行なうコンピュータは、複数の相手と同時に通信したり、複数の通信アプリケーションを同時に使用するために、補助アドレスとして複数のポートを持っています。
ポート転送	(Port Forwarding) WAN側のポート番号とプロトコル種別に対して、LAN側に接続された機器のIPアドレスとポート番号を静的に対応付ける機能です。これにより、LAN側に位置するWebサーバをWAN側に開示するといったサーバホスティングが可能になります。
ポート番号	(Port Number) 複数の相手と同時に接続を行うためにIPアドレスの下に設けられた補助アドレスです。ポートの指定には0から65535までの数字が使われます。この数値は一般的に「ポート番号」と呼ばれています。
ホスト名	(Host Name) ネットワークに接続されている機器を識別しやすくするため、機器に付加する名前です。英数字で数文字を設定することが多い。DNSサーバによりIPアドレスと対応付けられています。

【ま行】

マルチセッション	(Multisession) ネットワークまたはリモートコンピュータに複数接続している状態を意味します。

【ら行】

ルータ	(Router) LANどうしやLANとWANを接続するための中継装置です。
ルーティング	(Routing) パケットを宛先に届けるための経路を選択する機能です。
ルーティングテーブル	(Routing Table) ルーティングの際に参照するデータです。このデータにもとづいてルーティングを実行します。
レジスタサーバ	(Register Server) 各装置からの登録情報を受け付け、データベースに登録されている装置情報を更新するサーバです。

索引

アルファベット

ANY接続 ……3-11
CALLTBL状態 ……2-52
DHCPサーバ機能 ……2-14
DHCP設定 ……2-14
DSP状態 ……2-52
ESSID ……3-11
FQDN ……2-46
IPアドレス ……2-14
IP電話回線状態 ……2-52
IP電話サービス ……2-44
IP電話設定情報 ……2-46
IP電話着信拒否電話番号 ……2-44
LANインタフェース ……2-27
LAN側サブネットマスク ……2-9
LAN側転送IPアドレス ……2-18
LAN側転送ポート ……2-18
Lモード ……2-45,5-4
MACアドレス ……2-53
MTU値 ……2-12
NetBIOS ……5-7
NTPサーバ ……2-9
Ping送信 ……2-63
PPPoE ……2-11
PPPoE状態（接続先1～5） ……2-53
PSK（事前共有キー） ……3-6
REGISTERサーバアドレス ……2-46
REGISTERサーバポート番号 ……2-46
SIPドメイン名 ……2-46
SLIC状態 ……2-52
TCPステルスモード ……2-34
TKIP+PSK ……3-7
UDPステルスモード ……2-34
Unnumbered接続 ……1-3,1-12,2-13
UPnP機能 ……1-5,2-17
WANインタフェース ……2-27
WAN側IPアドレス ……2-9
WAN側サブネットマスク ……2-9
WAN側ポート ……2-9
WEP ……3-6
WEPキー ……3-9
Windows共有フィルタ ……5-7
WPA ……3-6

五十音

【ア行】

宛先ネットワークアドレス ……2-22
暗号化 ……3-7
インフラストラクチャ・モード ……3-20
オンライン登録 ……2-6

【カ行】

加入電話回線種別 ……2-43
簡易DMZ ……2-17
キーリフレッシュタイマ ……3-7
機能仕様 ……5-2
共有フィルタ／ステルス設定 ……2-34
ゲートウェイIPアドレス ……2-22
固定IP ……1-12,2-9,2-15

【サ行】

再起動 ……2-2,2-64
サブセッション ……2-24
出力インタフェース ……2-20
障害ログ表示 ……2-58
状態表示1 ……2-2,2-48
状態表示2 ……2-2,2-51

索引

セキュリティ ……………………2-39
接続パスワード ……………………2-12
接続ユーザ名 ……………………2-12
設定
DHCP設定 ……………………2-14
Dynamic DNS設定 ……………………2-32
IPフィルタ設定 ……………………2-20
MACアドレスフィルタリング ……2-37
NAPT設定 ……………………2-17
PPPoE設定 ……………………2-11
RIP設定 ……………………2-27
SPI設定 ……………………2-30
VPNパススルー設定 ……………………2-28
Windows共有フィルタ／
ステルス設定 ……………………2-34
アップデート設定 ……………………2-41
暗号化設定 ……………………2-36
ウイルス対策設定 ……………………2-40
かんたん設定 ……………………2-6
基本設定 ……………………2-36
サービス設定 ……………………2-43
セキュリティ ……………………2-39
電話設定 ……………………2-42
ネットワーク設定 ……………………2-8
パスワード設定 ……………………2-62
無線LAN設定 ……………………2-35
ルータ設定 ……………………2-7
ルーティングテーブル設定 ……2-22,2-24
設定記入シート ……………………5-27
設定値表示 ……………………2-63
設定例
音声／ビデオチャット等のソフトを
利用するときには ……………………1-5
外部にサーバを公開するには ……1-10
複数の固定IPアドレスを
利用するには ……………………1-12

【タ行】

追加する宛先ネットワークアドレス …2-25
追加するドメイン名 ……………………2-24
通話ログ表示 ……………………2-58
デフォルトゲートウェイ ……………………2-9
トラブルや疑問点がある場合 …………4-2

【ナ行】

入力インタフェース ……………………2-20
ネゴシエーション ……………………2-9

【ハ行】

バージョンアップ ……………………4-10
プログラム更新 ……………………4-10
プロトコル種別 ……………………2-18,2-20
プロバイダ（ISP） ……………………1-2,2-46
保守 ……………………2-2,2-61

【マ行】

無線LAN ……………………3-1
メインセッション ……………………2-22

【ヤ行】

用語集 ……………………5-12

【ラ行】

ログ表示 ……………………2-5,2-57

【ワ行】

割り込み音 ……………………2-44

設定記入シート

保守のための資料として、設定内容を記入し、大切に保管してください。
プロバイダの認証パスワードは、お客様の個人情報となります。
記入された際は、本設定記入シートのお取り扱いにご注意ください。

	設定項目	項目名	設定データ
初期設定	Web設定ログインパスワード	新しいパスワード	
	フレッツ・スクウェア接続設定	エリア設定	
ファームウェア更新確認情報設定	動作モード	動作モード	
	インターネットサービスプロバイダ設定	接続ユーザ名	
		接続パスワード	
	自動アップデート機能設定	実行時刻	指定なし／指定あり 時　分

メニュー	サブメニュー	設定項目	項目名	設定データ
かんたん設定	ー	セキュリティ設定	e-mailアドレス	
			通知する情報	□ソフトウェアのアップデート □ハッカーの侵入情報
		インターネットサービスプロバイダ設定	接続ユーザ名	(☛ファームウェア更新確認情報設定参照)
			接続パスワード	(☛ファームウェア更新確認情報設定参照)
		利用中電話サービス	ナンバー・ディスプレイ	あり／なし
			キャッチホン	あり／なし
ルータ設定	ネットワーク設定	動作モード	動作モード	PPPoE／DHCP／固定IP
		WAN側ネットワーク設定	WAN側IPアドレス/マスク長	／
			デフォルトゲートウェイ	
		DNSリレー設定(PPPoE利用時以外有効)	DNSサーバIPアドレス	プライマリ：セカンダリ：
		NTPサーバ設定	NTPサーバIPアドレス	
		LAN側ネットワーク設定	LAN側IPアドレス/マスク長	／
		IPv6ブリッジ設定	IPv6ブリッジ設定	無効／有効

（次ページに続く）

設定記入シート

<table>
<tr><th>メニュー</th><th>サブメニュー</th><th colspan="2">設定項目</th><th colspan="2">項目名</th><th>設定データ</th></tr>
<tr><td rowspan="18">ルータ設定</td><td rowspan="5">ネットワーク設定</td><td colspan="2" rowspan="5">ポート設定</td><td colspan="2">WANポート設定</td><td>自動認識/100M全二重/100M半二重/10M全二重/10M半二重</td></tr>
<tr><td colspan="2">LAN1ポート設定</td><td>自動認識/100M全二重/100M半二重/10M全二重/10M半二重</td></tr>
<tr><td colspan="2">LAN2ポート設定</td><td>自動認識/100M全二重/100M半二重/10M全二重/10M半二重</td></tr>
<tr><td colspan="2">LAN3ポート設定</td><td>自動認識/100M全二重/100M半二重/10M全二重/10M半二重</td></tr>
<tr><td colspan="2">LAN4ポート設定</td><td>自動認識/100M全二重/100M半二重/10M全二重/10M半二重</td></tr>
<tr><td rowspan="13">PPPoE設定</td><td colspan="2" rowspan="3">セッション設定</td><td colspan="2">契約セッション数</td><td></td></tr>
<tr><td colspan="2">メインセッション</td><td>接続先1/接続先2/接続先3/接続先4/接続先5</td></tr>
<tr><td colspan="2">使用するセッション</td><td>接続先1/接続先2/接続先3/接続先4/接続先5</td></tr>
<tr><td rowspan="10">インターネットサービスプロバイダ設定</td><td rowspan="10">接続先1</td><td colspan="2">接続ユーザ名</td><td></td></tr>
<tr><td colspan="2">接続パスワード</td><td></td></tr>
<tr><td colspan="2">認証方式</td><td>認証なし/PAP/CHAP/PAP+CHAP</td></tr>
<tr><td colspan="2">無通信監視タイマ</td><td>無効/1分/5分/10分/30分</td></tr>
<tr><td colspan="2">DNSサーバアドレス</td><td>プライマリ：
セカンダリ：</td></tr>
<tr><td colspan="2">MTU値</td><td></td></tr>
<tr><td colspan="2">IPアドレス指定</td><td>指定しない／指定する（unnumbered接続）</td></tr>
<tr><td></td><td>IPアドレス</td><td></td></tr>
<tr><td></td><td>マスク長</td><td></td></tr>
</table>

メニュー	サブメニュー	設定項目		項目名		設定データ
ルータ設定	PPPoE設定	インターネットサービスプロバイダ設定	接続先2	接続ユーザ名		
				接続パスワード		
				認証方式		認証なし/PAP/CHAP/PAP+CHAP
				無通信監視タイマ		無効/1分/5分/10分/30分
				DNSサーバアドレス		プライマリ： セカンダリ：
				MTU値		
				IP アドレス指定		指定する／指定しない（unnumbered接続）
					IPアドレス	
					マスク長	
			接続先3	接続ユーザ名		
				接続パスワード		
				認証方式		認証なし/PAP/CHAP/PAP+CHAP
				無通信監視タイマ		無効/1分/5分/10分/30分
				DNSサーバアドレス		プライマリ： セカンダリ：
				MTU値		
				IPアドレス指定		指定しない／指定する（unnumbered接続）
					IPアドレス	
					マスク長	

（次ページに続く）

設定記入シート

メニュー	サブメニュー	設定項目	項目名	設定データ
ルータ設定	PPPoE設定	インターネットサービスプロバイダ設定 接続先4	接続ユーザ名	
			接続パスワード	
			認証方式	認証なし/PAP/CHAP/PAP+CHAP
			無通信監視タイマ	無効/1分/5分/10分/30分
			DNSサーバアドレス	プライマリ： セカンダリ：
			MTU値	
			IPアドレス指定	指定しない／指定する（unnumbered接続）
			IPアドレス	
			マスク長	
		接続先5：フレッツ・スクウェア接続設定	無通信監視タイマ	1分/5分/10分/30分
	DHCP設定	LAN側ネットワーク設定	LAN側 IPアドレス／マスク長／	／
		DHCPサーバ設定	DHCPサーバ機能	有効/無効
			割り当て開始IPアドレス	
			割り当て終了IPアドレス	
			DNSサーバアドレス	
		固定IPアドレスで使用する端末の情報設定	IPアドレス	（☛P5-38参照）
			MACアドレス	

メニュー	サブメニュー	設定項目	項目名	設定データ
ルータ設定	NAPT設定	ー	動的NAPT機能	有効/無効
		ー	簡易DMZ IPアドレス	
		UPnP設定	UPnP機能	無効/接続先1 有効/接続先2 有効/接続先3 有効/接続先4有効/接続先5 有効
		静的NAPT設定 (ポート転送規則)	割り当て WAN側 受信ポート範囲	(☛P5-39参照)
			プロトコル種別	
			LAN側 転送 IPアドレス	
			LAN側 転送 ポート	
	IPフィルタ設定	ー	デフォルトの規則	許可/破棄
		パケットフィルタ規則	方針 (POLICY)	(☛P5-40～P5-47参照)
			プロトコル種別 (PROTOCOL)	
			入力インタフェース (IN)	
			出力インタフェース (OUT)	
			送信元IPアドレス／ マスク長 (SOURCE IP/MASK)	
			送信先IPアドレス／ マスク長 (DESTINATION IP/MASK)	
			送信先ポート番号 (PORT)	
	ルーティングテーブル設定 ルーティング条件(メインセッション)	スタティックルーティング設定	宛先ネットワークアドレス／マスク長	(☛P5-48参照)
			ゲートウェイ IPアドレス	

(次ページに続く)

設定記入シート

メニュー	サブメニュー	設定項目	項目名	設定データ
ルータ設定	ルーティングテーブル設定 ルーティング条件（サブセッション）	ー	追加するドメイン名	（☛P5-49参照）
		ー	追加する宛先ネットワークアドレス／マスク長	（☛P5-50参照）
	RIP設定	各インタフェースのRIP設定	LANインタフェース	有効／無効
			WANインタフェース	無効/接続先1 有効/接続先2 有効/接続先3 有効/接続先4有効
	VPNパススルー設定	PPTPパススルー設定(サーバ公開)	WANからLANへのアクセス	有効／無効
			LAN側IPアドレス	
			WAN側IPアドレス	すべて／指定 指定：
		IPsecパススルー設定(サーバ公開)	WANからLANへのアクセス	有効／無効
			LAN側IPアドレス	
			WAN側IPアドレス	すべて／指定 指定：
		L2TPパススルー設定(サーバ公開)	WANからLANへのアクセス	有効／無効
			LAN側IPアドレス	
			WAN側IPアドレス	すべて／指定 指定：

メニュー	サブメニュー	設定項目	項目名	設定データ
ルータ設定	SPI（ステートフルパケットインスペクション）設定	タイムアウト設定	ICMP	秒
			UDPアイドル	秒
			UDP STREAM	秒
			TCP ESTABLISHED	秒
			TCP SYNSENT	秒
			TCP SYNRECV	秒
			TCP FINWAIT	秒
			TCP TIMEWAIT	秒
			TCP CLOSE	秒
			TCP CLOSEWAIT	秒
			TCP LASTACK	秒
			TCP LISTEN	秒
		TCPセッション制限	セッション数	(☛P5-51参照)
			TCPポート番号	
	Dynamic DNS設定	Dynamic DNS設定	Dynamic DNS設定	有効／無効
			認証方法	なし／BASIC認証
			認証ID	
			認証パスワード	
			更新タイマ	時間
		Dynamic DNS URL設定	登録先URL	
	Windows共有フィルタ／ステルス設定	ー	Windows共有フィルタ	有効／無効
		ステルスモード設定	TCPステルスモード	有効／無効
			UDPステルスモード	有効／無効
			ICMPステルスモード	有効／無効

（次ページに続く）

設定記入シート

メニュー	サブメニュー	設定項目	項目名	設定データ
無線LAN設定	基本設定	ー	無線動作モード	11b+g／11g／11a
			ESSID	
			ANY接続	拒否／許可
			送信パワー設定	100／50／25（%）
		無線チャンネル	2.4 GHz帯	1(チャンネル)／ 2(チャンネル)／ 3(チャンネル)／ 4(チャンネル)／ 5(チャンネル)／ 6(チャンネル)／ 7(チャンネル)／ 8(チャンネル)／ 9(チャンネル)／ 10(チャンネル)／ 11(チャンネル)／ 12(チャンネル)／ 13(チャンネル)／
			5.0 GHz帯	34(チャンネル)／ 38(チャンネル)／ 42(チャンネル)／ 46(チャンネル)／
		速度設定	11b+g	auto
			11g	auto 54(Mbps)／ 48(Mbps)／ 36(Mbps)／ 24(Mbps)／ 18(Mbps)／ 12(Mbps)／ 9(Mbps)／ 6(Mbps)／

メニュー	サブメニュー	設定項目	項目名	設定データ
無線LAN設定	基本設定	速度設定	11a	auto 54(Mbps)／ 48(Mbps)／ 36(Mbps)／ 24(Mbps)／ 18(Mbps)／ 12(Mbps)／ 9(Mbps)／ 6(Mbps)／
	暗号化設定	ー	暗号方式	OFF／WEP／ TKIP + PSK
		WEP	WEPキータイプ	自動設定（Pass Phrase）／直接入力
			暗号化ビット長	64／128
			WEPキー Pass Phrase	
		WEPキー設定情報	WEPキータイプ	16進数（HEX）入力／文字入力
			デフォルト送信キー	1／2／3／4
			WEPキー1	
			WEPキー2	
			WEPキー3	
			WEPキー4	
		WPA-PSK情報	PSK（事前共有キー）	
			キーリフレッシュタイマ	分
	MACアドレスフィルタリング	MACアドレスフィルタリング	MACアドレスフィルタリング	有効／無効
			デフォルトポリシー	拒否／許可
		フィルタリングするMACアドレスの情報設定	MACアドレス	(☛P5-51、P5-52参照)
			ポリシー	

（次ページに続く）

設定記入シート

メニュー	サブメニュー	設定項目	項目名	設定データ
セキュリティ	ウイルス対策設定	不正アクセス	不正アクセスレベル	高／中／低
		ウイルス関連	Eメールウイルス検索	有効／無効
			Webメール ウイルス検索	有効／無効
			ウイルス検出時の処理	駆除／削除／放置
			ウイルス駆除失敗時の処理	削除／放置
		通知関連	e-mailアドレス	
			通知する情報	□ソフトウェアのアップデート □ハッカーの侵入情報
	アップデート設定	アップデート関連	アップデート待機時間	0分／ 15分／ 30分／ 60分／ 120分／
			アップデート間隔	1時間／ 3時間／ 6時間／ 12時間／ 24時間／
		アップデートプロキシ情報	プロキシサーバ	未使用／使用
			ホスト名	
			ポート番号	
			認証	なし／あり
			認証用ユーザ名	
			認証用パスワード	

メニュー	サブメニュー	設定項目	項目名	設定データ
電話設定	サービス設定	ー	市外局番	
			加入電話回線種別	自動／PB／DP
			ダイヤル桁間タイマ	4秒／5秒／6秒／7秒／8秒
		利用中電話サービス	ナンバー・ディスプレイ	なし／あり
			キャッチホン	なし／あり
		IP電話サービス	IP電話サービス	有効／無効
			発信時番号通知	通知／非通知
			割り込み音	なし／あり
		ー	IP電話 着信拒否電話番号	(☛P5-53参照)
	IP電話設定情報	ー	SIPサーバアドレス	
			SIPサーバ ポート番号	
			REGISTERサーバ アドレス	
			REGISTERサーバ ポート番号	
			SIPドメイン名	
			ユーザID	
			パスワード	
			IP電話番号	
			市外局番	
			アップデート確認用 URL	
保守	自動アップデート	自動アップデート機能設定	実行時刻	指定あり／指定なし 時　分

（次ページに続く）

設定記入シート

1.固定IPで使用する端末の情報設定

登録番号	IPアドレス	MACアドレス	記事
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

2.静的NAPT設定（ポート転送規則）

登録番号	割り当てWAN側受信ポート範囲	プロトコル種別	LAN側転送IPアドレス	LAN側転送ポート	記事
1	～	TCP／UDP			
2	～	TCP／UDP			
3	～	TCP／UDP			
4	～	TCP／UDP			
5	～	TCP／UDP			
6	～	TCP／UDP			
7	～	TCP／UDP			
8	～	TCP／UDP			
9	～	TCP／UDP			
10	～	TCP／UDP			
11	～	TCP／UDP			
12	～	TCP／UDP			
13	～	TCP／UDP			
14	～	TCP／UDP			
15	～	TCP／UDP			
16	～	TCP／UDP			
17	～	TCP／UDP			
18	～	TCP／UDP			
19	～	TCP／UDP			
20	～	TCP／UDP			
21	～	TCP／UDP			
22	～	TCP／UDP			
23	～	TCP／UDP			
24	～	TCP／UDP			
25	～	TCP／UDP			
26	～	TCP／UDP			
27	～	TCP／UDP			
28	～	TCP／UDP			
29	～	TCP／UDP			
30	～	TCP／UDP			
31	～	TCP／UDP			
32	～	TCP／UDP			

設定記入シート

3.パケットフィルタ規則

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
1	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
2	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
3	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
4	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
5	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
6	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
7	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	
8	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　　／　　)	全て／指定／(　　／　　)	全て／指定／(　　～　　)	

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
9	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
10	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
11	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
12	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
13	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
14	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
15	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
16	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	

（次ページに続く）

設定記入シート

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
17	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
18	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
19	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
20	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
21	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
22	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
23	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
24	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
25	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
26	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
27	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
28	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
29	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
30	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
31	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	
32	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／（　／　）	全て／指定／（　／　）	全て／指定／（　～　）	

（次ページに続く）

設定記入シート

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
33	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
34	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
35	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
36	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
37	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
38	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
39	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
40	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
41	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
42	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
43	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
44	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
45	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
46	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
47	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
48	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	

（次ページに続く）

設定記入シート

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
49	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
50	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
51	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
52	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
53	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
54	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
55	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	
56	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(　／　)	全て／指定／(　／　)	全て／指定／(　～　)	

登録番号	方針	プロトコル種別	入力インタフェース	出力インタフェース	送信元IPアドレス/マスク長	送信先IPアドレス/マスク長	送信先ポート番号	記事
57	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
58	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
59	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
60	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
61	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
62	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
63	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	
64	許可／破棄	全て／TCP／UDP／ICMP	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／WAN／LAN／接続先1／接続先2／接続先3／接続先4／接続先5	全て／指定／(／)	全て／指定／(／)	全て／指定／(～)	

設定記入シート

4.ルーティングテーブル設定　ルーティング条件（メインセッション）

登録番号	宛先ネットワークアドレス/マスク長	ゲートウェイIPアドレス	記事
1	／		
2	／		
3	／		
4	／		
5	／		
6	／		
7	／		
8	／		
9	／		
10	／		
11	／		
12	／		
13	／		
14	／		
15	／		
16	／		

5.ルーティングテーブル設定　ルーティング条件（サブセッション）

登録番号	追加するドメイン名	接続先	記事
2		接続先1／接続先2／接続先3／接続先4／接続先5	
3		接続先1／接続先2／接続先3／接続先4／接続先5	
4		接続先1／接続先2／接続先3／接続先4／接続先5	
5		接続先1／接続先2／接続先3／接続先4／接続先5	
6		接続先1／接続先2／接続先3／接続先4／接続先5	
7		接続先1／接続先2／接続先3／接続先4／接続先5	
8		接続先1／接続先2／接続先3／接続先4／接続先5	
9		接続先1／接続先2／接続先3／接続先4／接続先5	
10		接続先1／接続先2／接続先3／接続先4／接続先5	
11		接続先1／接続先2／接続先3／接続先4／接続先5	
12		接続先1／接続先2／接続先3／接続先4／接続先5	
13		接続先1／接続先2／接続先3／接続先4／接続先5	
14		接続先1／接続先2／接続先3／接続先4／接続先5	
15		接続先1／接続先2／接続先3／接続先4／接続先5	
16		接続先1／接続先2／接続先3／接続先4／接続先5	

（次ページに続く）

設定記入シート

登録番号	追加する宛先ネットワークアドレス/マスク長	接続先	記事
1	／	接続先1／接続先2／接続先3／接続先4／接続先5	
2	／	接続先1／接続先2／接続先3／接続先4／接続先5	
3	／	接続先1／接続先2／接続先3／接続先4／接続先5	
4	／	接続先1／接続先2／接続先3／接続先4／接続先5	
5	／	接続先1／接続先2／接続先3／接続先4／接続先5	
6	／	接続先1／接続先2／接続先3／接続先4／接続先5	
7	／	接続先1／接続先2／接続先3／接続先4／接続先5	
8	／	接続先1／接続先2／接続先3／接続先4／接続先5	
9	／	接続先1／接続先2／接続先3／接続先4／接続先5	
10	／	接続先1／接続先2／接続先3／接続先4／接続先5	
11	／	接続先1／接続先2／接続先3／接続先4／接続先5	
12	／	接続先1／接続先2／接続先3／接続先4／接続先5	
13	／	接続先1／接続先2／接続先3／接続先4／接続先5	
14	／	接続先1／接続先2／接続先3／接続先4／接続先5	
15	／	接続先1／接続先2／接続先3／接続先4／接続先5	
16	／	接続先1／接続先2／接続先3／接続先4／接続先5	

6.SPI（ステートフルパケットインスペクション）設定　TCPセッション制限

登録番号	セッション数	TCPポート番号	記事
1		ALL／ポート番号指定（　　）	
2		ALL／ポート番号指定（　　）	
3		ALL／ポート番号指定（　　）	
4		ALL／ポート番号指定（　　）	
5		ALL／ポート番号指定（　　）	
6		ALL／ポート番号指定（　　）	
7		ALL／ポート番号指定（　　）	
8		ALL／ポート番号指定（　　）	
9		ALL／ポート番号指定（　　）	
10		ALL／ポート番号指定（　　）	
11		ALL／ポート番号指定（　　）	
12		ALL／ポート番号指定（　　）	
13		ALL／ポート番号指定（　　）	
14		ALL／ポート番号指定（　　）	
15		ALL／ポート番号指定（　　）	
16		ALL／ポート番号指定（　　）	

7.フィルタリングするMACアドレスの情報設定

登録番号	MACアドレス	ポリシー	記事
1		拒否／許可	
2		拒否／許可	
3		拒否／許可	
4		拒否／許可	
5		拒否／許可	
6		拒否／許可	
7		拒否／許可	
8		拒否／許可	
9		拒否／許可	
10		拒否／許可	
11		拒否／許可	
12		拒否／許可	
13		拒否／許可	
14		拒否／許可	

（次ページに続く）

設定記入シート

登録番号	MACアドレス	ポリシー	記事
15		拒否／許可	
16		拒否／許可	
17		拒否／許可	
18		拒否／許可	
19		拒否／許可	
20		拒否／許可	
21		拒否／許可	
22		拒否／許可	
23		拒否／許可	
24		拒否／許可	
25		拒否／許可	
26		拒否／許可	
27		拒否／許可	
28		拒否／許可	
29		拒否／許可	
30		拒否／許可	
31		拒否／許可	
32		拒否／許可	

8.IP電話　着信拒否電話番号

登録番号	IP電話　着信拒否電話番号	記事
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

注　意
本商品は、外国為替および外国貿易法が定める規制貨物に該当いたします。
本商品は、国内でのご利用を前提としたものでありますので、日本国外へ持ち出す場合は、同法に基づく輸出許可等必要な手続きをお取りください。

NOTICE
This product, which is intended for use in Japan, is a controlled product regulated under the Japanese Foreign Exchange and Foreign Trade Law. When you plan to export or take this product out of Japan, please obtain a permission, as required by the Law and related regulations, from the Japanese Government.

当社ホームページでは、各種商品の最新の情報やバージョンアップサービスなどを提供しています。本商品を最適にご利用いただくために、定期的にご覧いただくことをお勧めします。

当社ホームページ： **【NTT東日本】http://www.east-plus.com/**
【NTT西日本】http://www.ntt-west.co.jp/kiki/

フレッツ・セーフティに関するホームページ：
【NTT東日本】http://flets.com/safety/
【NTT西日本】http://flets-w.com/safety/

使い方でご不明の点がございましたら、下記へお気軽にご相談ください。

■NTT東日本エリア（北海道、東北、関東、甲信越地区）でご利用のお客様

●本商品の取り扱いに関するお問い合わせ
0120－970413　(9:00〜21:00)
携帯電話・PHS・050IP電話からご利用の場合（通話料金がかかります）
03－5667－7100　(9:00〜21:00)
※年末年始12月29日〜1月3日は休業とさせていただきます。

●故障に関するお問い合わせ
0120－242751　(24時間　年中無休※)
※故障修理等の対応時間は平日9：00〜17：00
土・日・祝日および年始1月1日〜1月3日は休業とさせていただきます。

●フレッツ・セーフティおよびセキュリティに関するお問い合わせ
03－5442-7533　(9:00〜17:00)
※土・日・祝日および年末年始12月29日〜1月3日は休業とさせていただきます。

■NTT西日本エリア（東海、北陸、近畿、中国、四国、九州地区）でご利用のお客様

●本商品の取り扱いに関するお問い合わせ
0120－109217（トークニイーナ）　(9:00〜17:00)
※年末年始12月29日〜1月3日は休業とさせていただきます。

●故障に関するお問い合わせ
0120－248995　(24時間　年中無休)
※携帯電話・PHSからもご利用になれます。

●セキュリティに関するお問い合わせ
0120－248303　(9:00〜17:00)
※年末年始12月29日〜1月3日は休業とさせていただきます。

電話番号をお間違えにならないように、ご注意願います。

本2581-4 (2005.10)
SEC-WBC3 <X400V>トリセツ
Rev2.1